D-Link®
Building Networks for People

## DGS-1210-10P

# MANUAL
## WEB SMART SWITCH

WIRED

## *Table of Contents*

**Table of Contents ..... i**
**About This Guide ..... 1**
Terms/Usage ..... 1
Copyright and Trademarks ..... 1
**Product Introduction ..... 2**
DGS-1210-10P ..... 3
Front Panel ..... 3
Rear Panel ..... 3
**Hardware Installation ..... 4**
Step 1: Unpacking ..... 4
Step 2: Switch Installation ..... 4
Desktop or Shelf Installation ..... 4
Rack Installation ..... 4
Step 3 – Plugging in the AC Power Cord ..... 5
Power Failure ..... 6
**Getting Started ..... 7**
Management Options ..... 7
Using Web-based Management ..... 7
Supported Web Browsers ..... 7
Connecting to the Switch ..... 7
Login Web-based Management ..... 8
Smart Wizard ..... 8
Web-based Management ..... 8
SmartConsole Utility ..... 8
**SmartConsole Utility ..... 10**
SmartConsole Settings ..... 10
Utility Settings ..... 10
Log ..... 11
Trap ..... 11
File ..... 11
Help ..... 12
Device Configuration ..... 13
Add(+), Delete(-) and Discover the device ..... 15
Device List ..... 15
**Configuration ..... 17**
Smart Wizard Configuration ..... 17
Password Settings ..... 17
SNMP Settings ..... 18
System Settings ..... 19
Web-based Management ..... 20
Tool Bar > Save Menu ..... 21
Save Configuration ..... 21
Save Log ..... 21
Tool Bar > Tool Menu ..... 21
Reset ..... 21
Reset System ..... 21
Reboot Device ..... 22

Configuration Backup & Restore ..... 22
Firmware Backup and Upload ..... 22
Tool Bar > Smart Wizard ..... 23
Tool Bar > Online Help ..... 23
Function Tree ..... 25
Device Information ..... 25
System > System Settings ..... 26
System > Trap Settings For SmartConsole ..... 27
System > Port Settings ..... 27
System > SNMP Settings ..... 28
System > Password Access Control ..... 29
System > System Log Settings ..... 29
Configuration > Jumbo Frame ..... 30
Configuration > 802.1Q VLAN ..... 30
Configuration > Asymmetric VLAN ..... 31
Configuration > 802.1Q Management VLAN ..... 33
Configuration > Voice VLAN > Voice VLAN Setting ..... 33
Configuration > Voice VLAN > Voice VLAN OUI Setting ..... 34
Configuration > Link Aggregation > Port Trunking ..... 35
Configuration > Link Aggregation > LACP Port Settings ..... 36
Configuration > IGMP Snooping ..... 36
Configuration > Port Mirroring ..... 38
Configuration > Power Saving ..... 38
Configuration > Loopback Detection ..... 38
Configuration > SNTP Settings > Time Settings ..... 39
Configuration > SNTP Settings > TimeZone Settings ..... 40
Configuration > Spanning Tree > STP Global Settings ..... 40
Configuration > Spanning Tree > STP Port Settings ..... 41
QoS > Storm Control ..... 43
QoS > Bandwidth Control ..... 43
QoS > 802.1p/DSCP Priority Settings ..... 44
Security > Trusted Host ..... 45
Security > Safeguard Engine ..... 46
Security > Port Security ..... 46
Security > 802.1X > 802.1X Settings ..... 46
Security > MAC Address Table > Static MAC ..... 48
Security > MAC Address Table > Dynamic Forwarding Table ..... 48
Monitoring > Statistics ..... 49
Monitoring > Cable Diagnostics ..... 50
Monitoring > System Log ..... 50
ACL > ACL Configuration Wizard ..... 51
ACL > ACL Profile List ..... 52
ACL > ACL Finder ..... 55
PoE > PoE Port Settings ..... 55
PoE > PoE System Settings ..... 56
Time-Based PoE > Time Range Settings ..... 57
LLDP > LLDP Global Settings ..... 57
LLDP > LLDP Remote Port Information ..... 58
LLDP > LLDP MED Settings ..... 58

**Command Line Interface ..... 59**
To connect a switch via TELNET: ..... 59
Logging on to the Command Line Interface: ..... 59
CLI Commands: ..... 59
Download ..... 59
Upload ..... 60
Config ipif System ..... 60
Logout ..... 60
Ping ..... 61
Reboot ..... 61
Reset ..... 61
Show ipif ..... 61
Show switch ..... 61
Config account admin password ..... 62
Save ..... 62
**Appendix A - Ethernet Technology ..... 63**
Gigabit Ethernet Technology ..... 63
Fast Ethernet Technology ..... 63
Switching Technology ..... 63
**Appendix B - Technical Specifications ..... 62**
Hardware Specifications ..... 62
Key Components / Performance ..... 62
Port Functions ..... 62
Physical & Environment ..... 62
Emission (EMI) Certifications ..... 62
Safety Certifications ..... 62
Features ..... 62
L2 Features ..... 62
D-Link Green Technology ..... 62
VLAN ..... 63
QoS (Quality of Service) ..... 63
Security ..... 63
Management ..... 63
**Appendix C – Rack mount Instructions ..... 64**

## About This Guide

This guide provides instructions to install the D-Link Gigabit Web Smart PoE Switch DGS-1210-10P, how to use the SmartConsole Utility, and to configure Web-based Management step-by-step.

**Note:** The model you have purchased may appear slightly different from the illustrations shown in the document. Refer to the Product Instruction and Technical Specification sections for detailed information about your switch, its components, network connections, and technical specifications.

This guide is mainly divided into four parts:

1. Hardware Installation: Step-by-step hardware installation procedures.
2. Getting Started: A startup guide for basic switch installation and settings.
3. Smart Console Utility: An introduction to the central management system.
4. Configuration: Information about the function descriptions and configuration settings.

### Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to the Smart Switch, and “switch” (first letter lower case) refers to other Ethernet switches. Some technologies refer to terms “switch”, “bridge” and “switching hubs” interchangeably, and both are commonly accepted for Ethernet switches.

A **NOTE** indicates important information that helps a better use of the device.

A **CAUTION** indicates potential property damage or personal injury.

### Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2009 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

# 1 *Product Introduction*

Thank you and congratulations on your purchase of D-Link Web Smart Switch Products.

D-Link's next generation Web Smart Ethernet switch series blends plug-and-play simplicity with exceptional value and reliability for small and medium-sized business (SMB) networking. All models are housed in a new style rack-mount metal case with easy-to-view front panel diagnostic LEDs, and provides advance features including two combo 100/1000BASE-X SFP slots for fiber connection, network security, traffic segmentation, QoS and versatile management.

***Power over Ethernet.*** DGS-1210-10P is compliant with 802.3af and the pre-standard of 802.3at, which provides the ability to run power over network cables at network sites. First eight 10/100/1000BASE-T Ethernet ports of this switch are selectable to provide up to 15.4 or 30 watts power for connected wireless access points, IP phones and other PoE-supported devices, allowing them to be deployed at difficult places such as on high walls and ceilings, where AC power outlets are not readily available.

***D-Link Green Technology.*** D-Link Green devices are about providing eco-friendly alternatives without compromising performance. D-Link Green Technology includes a number of innovations to reduce energy consumption on DGS-1210 series such as reducing power when a port does not have a device attached, or adjusting the power usage according to the Ethernet cable connected to it. For PoE model such as DGS-1210-10P, D-Link Green Technology offers Time-based PoE feature to shut down per port power off working hours.

***Extensive Layer 2 Features.*** Implemented as complete L2 devices, these switches include functions such as IGMP snooping, port mirroring, Spanning Tree, 802.3ad LACP and Loopback Detection to enhance performance and network resiliency.

***Traffic Segmentation and QoS.*** The switches support 802.1Q VLAN standard tagging to enhance network security and performance. The switches also support 802.1p priority queues, enabling users to run bandwidth-sensitive applications such as streaming multimedia by prioritizing that traffic in network. These functions allow switches to work seamlessly with VLAN and 802.1p traffic in the network. Auto Voice VLAN will automatically place the voice traffic from IP phone to an assigned VLAN with higher priority, so it can be separated from normal data traffic. Asymmetric VLAN is implemented in these switches for a more efficient use of shared resources, such as server or gateway devices.

***Network Security.*** D-Link's innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. Additional features like 802.1X port-based authentication provides access control of the network with external RADIUS servers. ACL is a powerful tool to screen unwanted IP or MAC traffic. Storm Control can help to keep the network from being overwhelmed by abnormal traffic. Port Security is another simple but useful authentication method to maintain the network device integrity.

***Versatile Management.*** The new generation of D-Link Web Smart Switches provides growing businesses with a simple and easy management of their network, using an intuitive SmartConsole utility or a Web-Based management interface that allows administrators to remotely control their network down to the port level. The SmartConsole easily allows customers to discover multiple D-Link web smart switches with the same L2 network segment connected to the user's local PC. With this utility, users do not need to change the IP address of the PC and provide easy initial settings of the smart switches. The switches within the same L2 network segment connected to the user's local PC are displayed on the screen for instant access. It allows extensive switch configuration settings, and basic configuration of discovered devices, such as a password change or firmware upgrade.

Users can also access the switch via TELNET. Some basic tasks can be performed such as changing the Switch IP address, resetting the settings to factory defaults, setting the administrator password, rebooting the Switch, or upgrading the Switch firmware by using the Command Line Interface (CLI).

In addition, users can utilize the SNMP MIB (*Management Information Base*) to poll the switches for information about the status, or send out traps of abnormal events. SNMP support allows users to integrate

the switches with other third-party devices for management in an SNMP-enabled environment. D-Link Web Smart Switches also come with the D-View plug-in module that works with D-View 6 SNMP Management Software, and provides easy-to-use graphic interface and facilitates the operation efficiency.

## *DGS-1210-10P*

8-Port 10/100/1000Mbps plus 2 1000Base-T/SFP ports Web Smart PoE Switch

### Front Panel

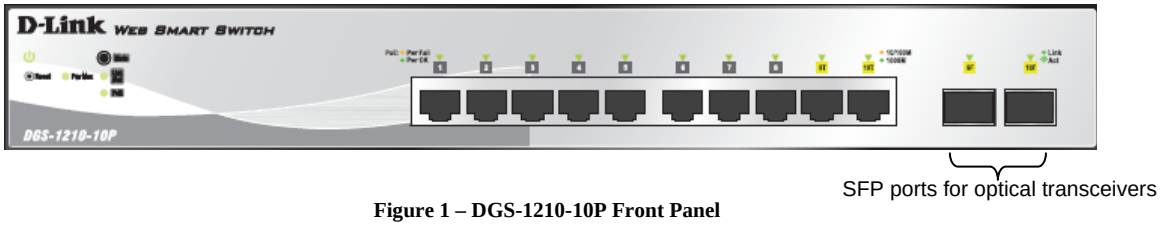


**Figure 1 – DGS-1210-10P Front Panel**

**Power LED :** The Power LED lights up when the Switch is connected to a power source.

**Pwr Max:** The Pwr Max LED lights up when the Switch reaches the maximum power budget defined by the administrator via PoE System Settings page of Web GUI or the default power budget of 78 Watts.

**Reset:** By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost.

**Mode:** By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.

**Port Link/Act/Speed LED (1-8, 9T, 10T, 9F, 10F):** When mode LED lights up in Link/Act mode, the port LEDs indicate a network link through the corresponding port. Blinking indicates the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 10M or 100M. When the port LED glows in green, it is running on 1000Mbps.

**NOTE:** On DGS-1210-10P, the SFP ports are shared with normal RJ-45 ports 9 to 10. When optical transceiver is inserted to SFP port and link up, the RJ-45 port cannot be used.

**Port PoE LED (1-8):** When mode LED lights up in PoE mode, the port LEDs indicate powering status over the corresponding port.

### Rear Panel

**Figure 2 – DGS-1210-10P Rear Panel**

**Power:** The power port is where to connect the AC power cord.

# 2 *Hardware Installation*

This chapter provides unpacking and installation information for the D-Link Web-Smart Switch.

## *Step 1: Unpacking*

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged. If any item is missing or damaged, please contact your local D-Link reseller for replacement.

- One D-Link Web-Smart Switch
- One AC power cord
- Four rubber feet
- Screws and two mounting brackets
- One Multi-lingual Getting Started Guide
- One CD with User Manual, SmartConsole Utility program, and D-View Module

If any item is found missing or damaged, please contact the local reseller for replacement.

## *Step 2: Switch Installation*

For safe switch installation and operation, it is recommended that you:

- Visually inspect the power cord to see that it is secured fully to the AC power connector.
- Make sure that there is proper heat dissipation and adequate ventilation around the switch.
- Do not place heavy objects on the switch.

### Desktop or Shelf Installation

When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it.

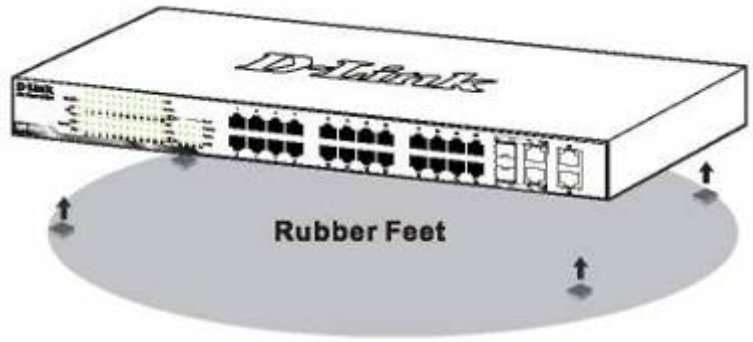


**Figure 3 – Attach the adhesive rubber pads to the bottom**

### Rack Installation

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided (please note that these brackets are not designed for palm size switches).

**Figure 4 – Attach the mounting brackets to the Switch**

Then, use the screws provided with the equipment rack to mount the switch in the rack.

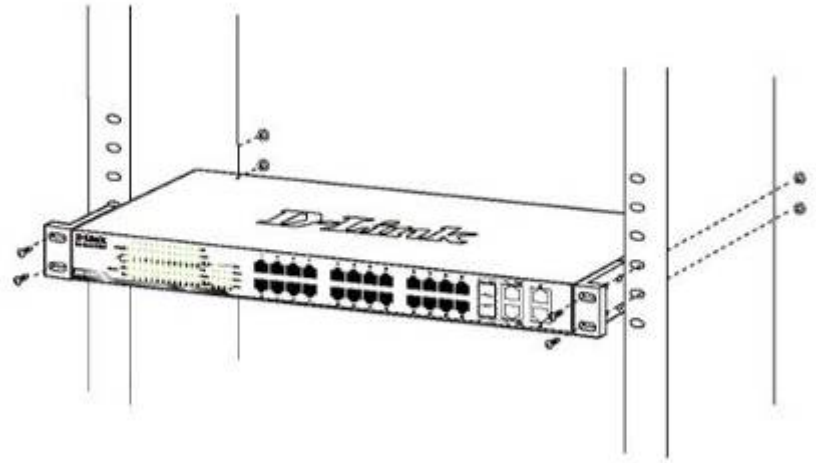

**Figure 5 – Mount the Switch in the rack or chassis**

Please be aware of following safety Instructions when installing:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit, and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

### *Step 3 – Plugging in the AC Power Cord*

Users may now connect the AC power cord into the rear of the switch and to an electrical outlet (preferably one that is grounded and surge protected).

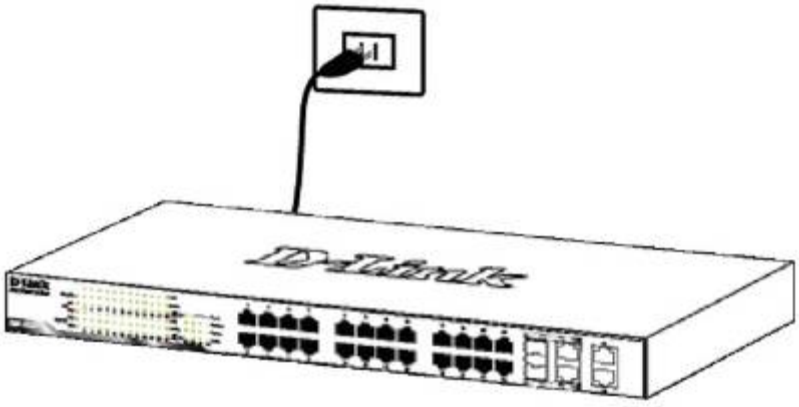

**Figure 6 –Plugging the switch into an outlet**

**Power Failure**

As a precaution, the switch should be unplugged in case of power failure. When power is resumed, plug the switch back in.

# 3 Getting Started

This chapter introduces the management interface of D-Link Web-Smart Switch.

## Management Options

The D-Link Web Smart Switch can be managed through any port on the device by using the Web-based Management, or through any PC using the SmartConsole Utility.

Each switch must be assigned its own IP Address, which is used for communication with the Web-Based Management or a SNMP network manager. The PC should have an IP address in the same range as the switch. Each switch can allow up to four users to access the Web-Based Management concurrently.

However, if you want to manage multiple D-Link Web Smart Switches, the SmartConsole Utility is a more convenient choice. By using the SmartConsole Utility, you do not need to change the IP address of your PC and it is easier to initialize multiple Smart Switches.

Please refer to the following installation instructions for the Web-based Management and the SmartConsole Utility.

## Using Web-based Management

After a successful physical installation, you can configure the Switch, monitor the network status, and display statistics using a web browser.

### Supported Web Browsers

The embedded Web-based Management currently supports the following web browsers:

- Internet Explorer 6 or higher
- Netscape 8 or higher
- Mozilla
- Firefox 1.5/2.0 or higher

### Connecting to the Switch

You will need the following equipment to begin the web configuration of your device:

1. A PC with a RJ-45 Ethernet connection
2. A standard Ethernet cable

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.

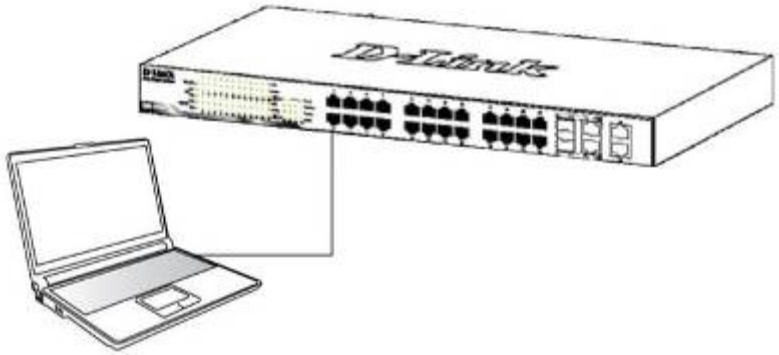

**Figure 7 –Connected Ethernet cable**

**Login Web-based Management**

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP address of **10.x.y.z** (where x/y is a number between 0 ~ 254 and z is a number between 1 ~ 254), and a subnet mask of **255.0.0.0**. There are two ways to launch the Web-based Management, you may either click the Web Access button at the top of the SmartConsole Utility or open the web browser and enter **10.90.90.90** (the factory-default IP address) in the address bar. Then press <Enter>.

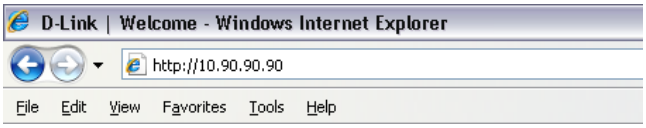


**Figure 8 –Enter the IP address 10.90.90.90 in the web browser**

**NOTE:** The switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

The web configuration can also be accessed through the SmartConsole Utility. Open the SmartConsole Utility and double-click the switch as it appears in the Monitor List. This will automatically load the web configuration in your web browser.

When the following logon dialog box appears, enter the password then click **OK**. The default password is **admin**.

**Figure 9 – Logon Dialog Box**

## *Smart Wizard*

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link Web Smart Switch. Please refer to the Smart Wizard Configuration section for details.

## *Web-based Management*

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface. Please refer to Chapter 5 Configuration for detailed instructions.

## *SmartConsole Utility*

The SmartConsole Utility included in the installation CD is a program for discovering D-Link Smart Switches within the same network segment connected to your PC. This tool is only for computers running Windows 2000, Windows XP, or Windows Vista x64/86 operating systems. There are two options for the installation of the SmartConsole Utility; one is through the autorun program on the installation CD and the other is manual installation.

**NOTE:** Please be sure to uninstall any existing SmartConsole Utility from your PC before installing the latest SmartConsole Utility.

**Option 1:** Follow these steps to install the SmartConsole Utility via the autorun program on the installation CD.

1. Insert the Utility CD into your CD-Rom/DVD-Rom Drive.
2. The autorun program will appear automatically.
3. Click on the ”Install SmartConsole Utility” button and an installation wizard will guide you through the process.
4. After successfully installing the SmartConsole Utility, you can open the utility by clicking Start > Programs > D-Link SmartConsole Utility.
5. Connect the Smart Switch to the same L2 network segment of your PC and use the SmartConsole Utility to discover the Smart Switches.

**Option 2:** Follow these steps to install the SmartConsole Utility manually.

1. Insert the Utility CD into your CD-Rom/DVD-Rom Drive.
2. From the Start menu on the Windows desktop, click Run.
3. In the Run dialog box, type D:\D-Link SmartConsole Utility\setup.exe (where D:\ represents the drive letter of your CD-Rom or DVD-Rom) and click OK.
4. Follow the on-screen instructions to install the utility.
5. Upon completion, go to Start > Programs > D-Link SmartConsole Utility and open the SmartConsole Utility.
6. Connect the Smart Switch to the same L2 network segment of your PC and use the SmartConsole Utility to discover the Smart Switches.

For detailed explanations of SmartConsole’s functions, please refer to Chapter 4 SmartConsole Utility

# 4 SmartConsole Utility

The D-Link SmartConsole Utility allows the administrator to quickly discover all D-Link smart switches, which are in the same domain of the PC, collect traps and log messages, and quick access to basic configurations of the switch.

The SmartConsole Utility consists of three parts, **Device Configurations** at the top, **Device List** as the main body, and **SmartConsole Settings** at the left.

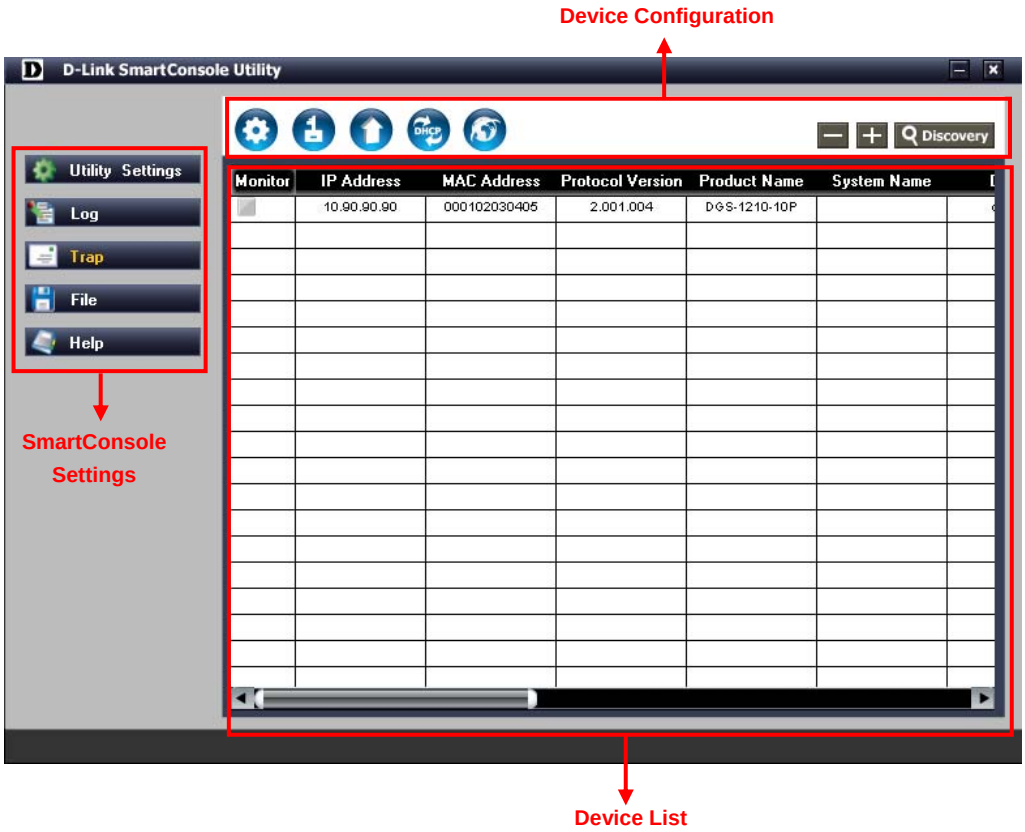


**Figure 10 – SmartConsole Utility**

## SmartConsole Settings

The SmartConsole Settings at the left has five icons, **Utility Settings**, **Log**, **Trap**, **File**, and **Help**.

### Utility Settings

Click this icon to launch the Utility Settings window. **Refresh time** refreshes the devices, which were selected as monitored devices in the Device List. Choices include **15 secs, 30 secs, 1 mins, 2 mins,** and **5 mins** for selecting the monitoring time intervals. **Utility Group Interval** establishes the intervals (in seconds) that the Switch will be discovered in the SmartConsole Device List.

**Figure 11 – SmartConsole Utility Settings**

**NOTE:** If the Group Interval is set to 0, IGMP Snooping must be disabled in the Switch, or the

Web-Smart Switch will not be discovered.

**Log**

Click this icon to launch the Log window. Click **View Log** to show the events of the SmartConsole Utility and the device. **Date/Time** indicates when the message was received, **IP** denotes where it comes from and **Status** shows the content of this log message. Click **Clear Log** to clear all log entries. Click **OK** to exit.

**Figure 12 – SmartConsole Log**

**Trap**

Click this icon to launch the Trap window. Click **View Trap** to show the events of the SmartConsole Utility and the device. **Date/Time** indicates when the trap message was received, **IP** denotes where it comes from and **Status** shows the content of this trap message. Click **Clear Trap** to clear all entries. Click **OK** to exit

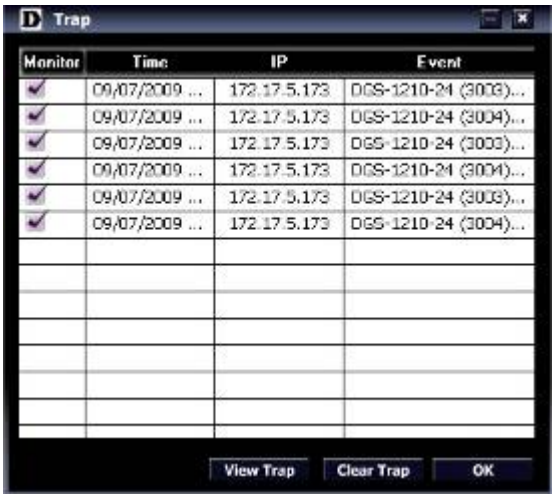


**Figure 13 – SmartConsole Trap**

The trap icon in the SmartConsole Settings will change while receiving new trap messages. Please see below for detailed description.

| Icon | Description |
|---|---|
| | No new traps |
| | New traps was received |

**File**

By clicking on this icon you will see below options:

**Figure 14 – SmartConsole File**

**Monitor Save:** Records the setting of the Device List as default for the next time the SmartConsole Utility is used.

**Monitor Save As:** Records the setting of the Device List in an appointed filename and file path.

**Monitor Load:** Manually load a Device List setting file.

**Help**

Click this icon to launch the SmartConsole Info window.

About D-Link SmartConsole Utility
D-Link SmartConsole Utility Version 2.10.01 Protocol Version 2.001.004 @ 2009 D-Link Corporation.All rights reserved
OK

**Figure 15 – SmartConsole Help**

## *Device Configuration*

The Device Configuration in the SmartConsole Utility has five icons:

Device Settings

Device Password Manager

Multi Firmware Upgrade

DHCP Refresh

Web Access

and the +, −, Discovery device buttons for the Device List.

### Device Settings

Select a switch from the Device List. Click on this icon to launch the Device Settings window. Here you can configure the Product Name, IP Address, Gateway, Subnet Mask, System Name, Location, Trap Host IP, Switch Group Interval, and DHCP Client Setting of the Switch.

To apply the configuration, insert the correct device password in the Confirm Password box and then click **OK**

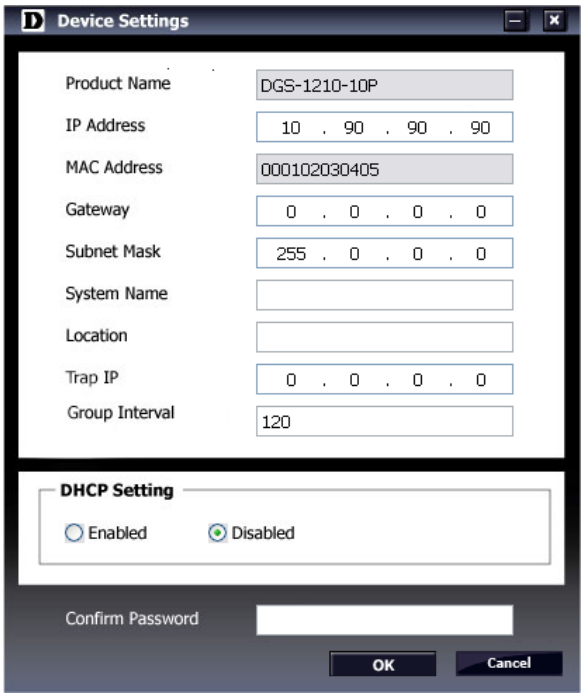


**Figure 16 – SmartConsole Device Settings**

## Device Password Manager

Select a switch from the Device List. Click on this icon to launch the Device Password Manager window. Here you can enter a new password and confirm it.

**Figure 17 – SmartConsole Device Password Manager**

## Multi Firmware Upgrade

Select one or many switches of the same model name from the Device List. Click on this icon to launch the Firmware Upgrade window. Specify the Firmware Path (or Browse for one) that you are going to use. Input the correct password of the device, and then click **Upgrade.** The state will show "OK" after completion, or "Fail" if the firmware upgrade fails or cannot be completed for any reason.

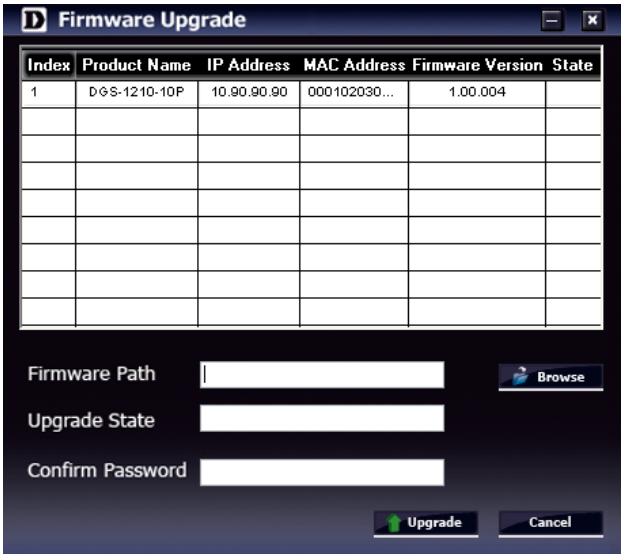


**Figure 18 – Firmware Upgrade**

**CAUTION:** Do not disconnect the PC or remove the power cord from the device until the upgrade completes. The software may be corrupted because of the incomplete firmware upgrade.

## DHCP Refresh:

If a DHCP-client enabled switch in the Device List shows the default IP is still used, it means the device did not receive an IP address from the DHCP server successfully. Select that switch and click the DHCP refresh icon. Enter the correct Device Password and then click **OK.** The device will renew the IP address from the DHCP server.

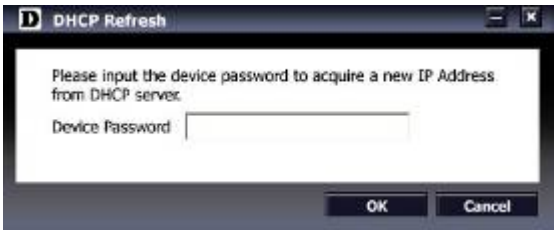


**Figure 19 – DHCP Refresh**

**Web Access**

Select a switch from the Device List. Click this icon to launch your Internet browser (eg. The Internet Explorer). Here you can configure the Switch through the Web-based Management utility. You may also get into the Web-based Management by double-clicking the device in the device list.

**Add(+), Delete(-) and Discover the device**

Click the **Discovery** button to display all of the Web-Smart devices located in the same domain with the management PC.

Click the **+** and insert a device IP address to add a device into the Discover List, or select a device and click the **–** button to remove it.

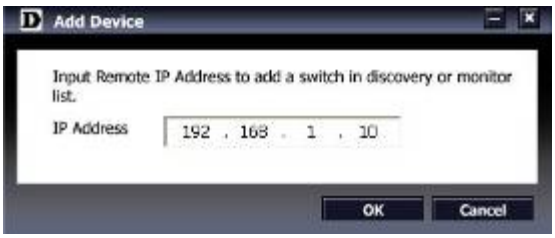


**Figure 20 – SmartConsole Add device**

**Figure 21 – SmartConsole Delete device**

## *Device List*

This list displays all discovered Web-Smart devices on the network.

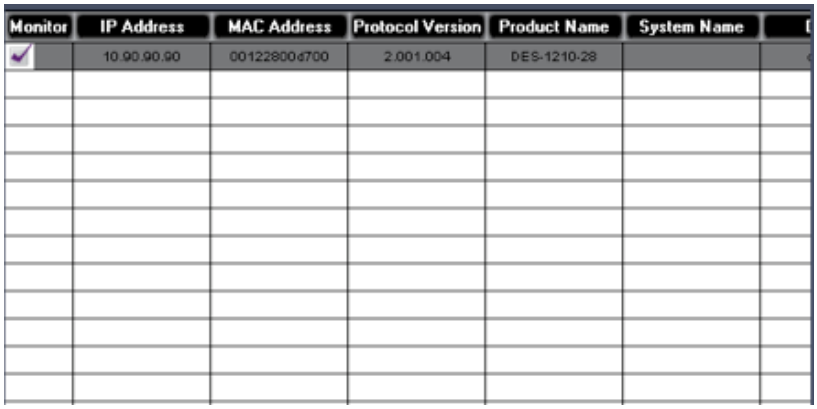


**Figure 22 – SmartConsole Device List**

Definitions of the Device List features:

**Monitor:** Checking the Monitor box and the SmartConsole will collect the trap and log data from the device. The in the monitor means the device was discovered by SmartConsole. Click the icon to have the device to continue updating the information, such as system log or trap to the SmartConsole Utility. The icon will appear . When the device was detected as not reachable, the icon will change to . Please check if the power or the cable of this device is disconnected.

**IP Address:** Displays the current IP addresses of devices.

**MAC Address:** Displays the device MAC Addresses.

**Protocol version:** Displays the software version of the Utility.

**Product Name:** Displays the device product name.

**System Name:** Displays the appointed device system name.

**DHCP:** Specify if the device gets the IP address from a DHCP server.

**Location:** Displays the location of the appointed device.

**Trap IP:** Displays the IP address of the host where the Trap information will be sent.

**Subnet Mask:** Displays the Subnet Mask setting of the device.

**Gateway:** Displays the Gateway setting of the device.

**Device Group Interval:** Displays the intervals (in seconds) that the Switch will be discovered in the SmartConsole Device List

**Firmware version:** Displays the current Firmware version of this device.

**LLDP**: Displays the LLDP (Link Layer Discovery Protocol*)* status of the device.

**SNMP**: Displays the SNMP status of the device.

**NOTE:** If the devices are marked red in the device list, it means that a firmware upgrade is required again.

**NOTE:** The LLDP function is only provided by PoE models. For non-PoE models, the LLDP column will appear blank.

# 5 *Configuration*

The features and functions of the D-Link Web Smart Switch can be configured for optimum use through the Web-based Management Utility.

## *Smart Wizard Configuration*

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link Web Smart Switch. If you do not plan to change anything, click **Exit** to leave the Wizard and enter the Web Interface. You can also skip it by clicking **Don't show Smart Wizard next time** for the next time you logon to the Web-based Management.

### Password Settings

Password setting allows you to change the login password of the device. Type the desired new password in the **Switch Password** box and again in the **Confirm Switch Password,** then click the **Apply** button to make it effective.

Welcome to Smart Wizard
The Smart Wizard will guide you to configure some functions all at once. If you are not planning to do any change in it, you can click exit to get out of the wizard and go back to Web Interface.
Password Settings
SNMP Settings
System Settings
Switch Password
Confirm Switch Password
Don't show Smart Wizard next time
Exit
Apply

**Figure 23 – Configure Password in Smart Wizard**

**SNMP Settings**

The SNMP Setting allows you to quickly enable/disable the SNMP function and configure the SNMP community name. For the complete SNMP function, please check “Setup Menu > System > SNMP Settings” in the Web Interface. The default SNMP Setting is Disabled. Click **Enabled,** enter Community names, and then click **Apply** to make it effective.

**Read_Only Community:** Read-only privilege allows authorized management stations to retrieve MIB objects values. Default Community name is **public**.

**Read_Write Community** Read/write privilege allows authorized management stations to retrieve and modify MIB object values. Default Community name is **private**.

**Figure 24 – Configure SNMP in Smart Wizard**

**System Settings**

You can manually change the system IP Address, Subnet Mask, and Gateway address by selecting **Static** and clicking **Apply**. You can further configure and read more about the above settings in the "Setup Menu > System > System Settings". The default setting of System IP address is Static. Select **DHCP** to have the switch obtain an IP address from a DHCP server in the network.

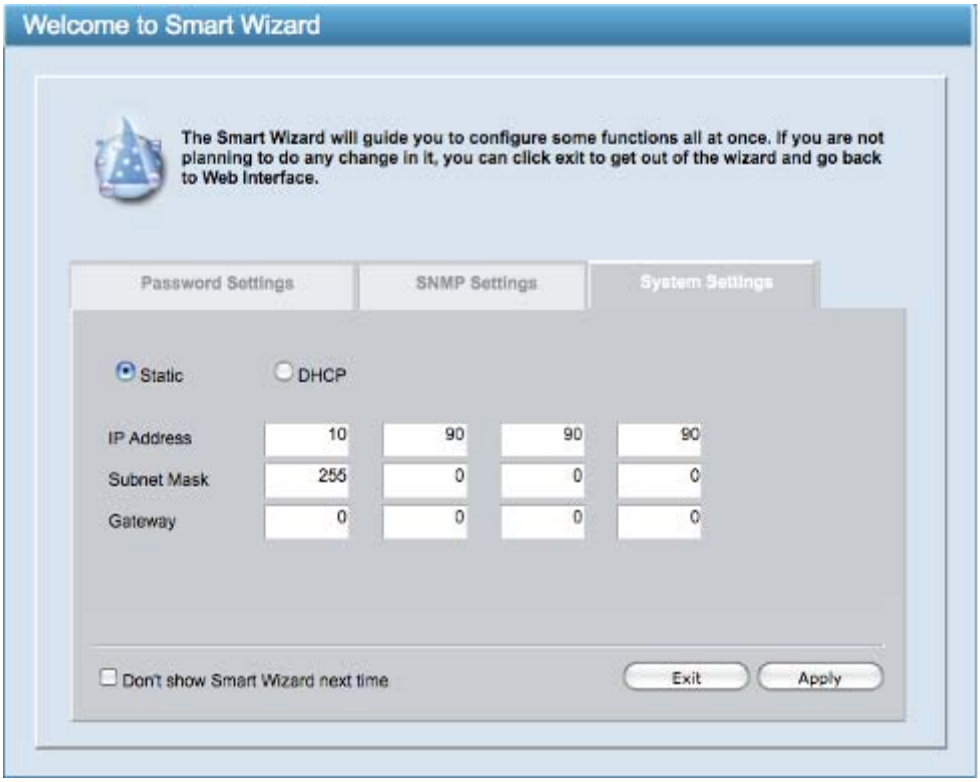


**Figure 25 – Configure System IP address in Smart Wizard**

**NOTE:** Changing the system IP address will disconnect you from the current connection. Please enter the correct IP address in the Web browser again and make sure your PC is in the same subnet with the switch. See Login Web-based Management for a detailed description.

If you want to change the IP settings, click **OK** and start a new web browser.

**Figure 26 – Confirm the changes of IP address in Smart Wizard**

## *Web-based Management*

After clicking the **Exit** button in Smart Wizard you will see the screen below:

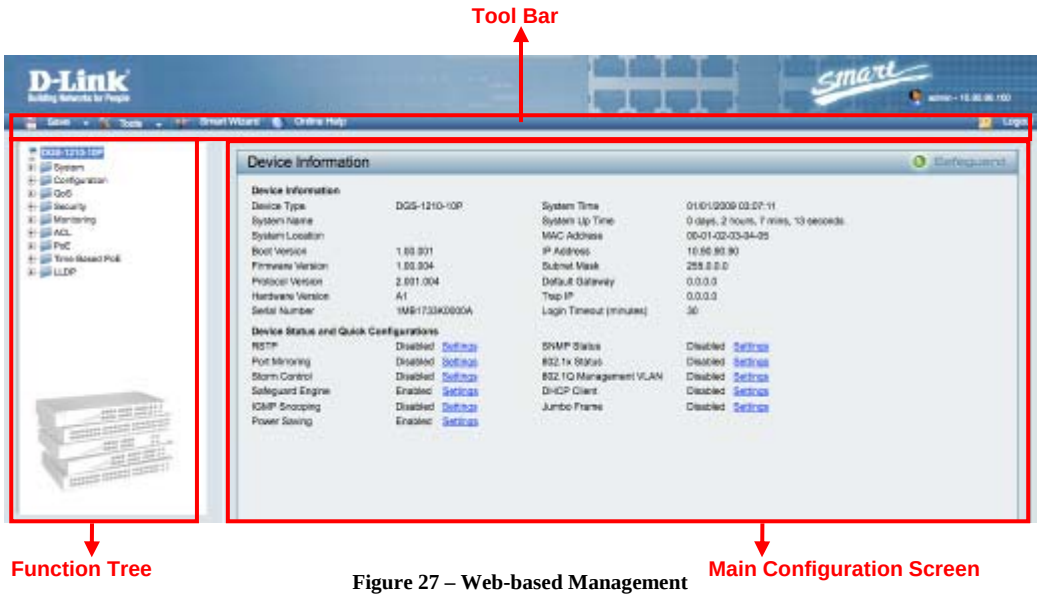


**Figure 27 – Web-based Management**

The above image is the Web-based Management screen. The three main areas are the **Tool Bar** on top, the **Function Tree**, and the **Main Configuration Screen**.

The **Tool Bar** provides a quick and convenient way for essential utility functions like firmware and configuration management.

By choosing different functions in the **Function Tree**, you can change all the settings in the **Main Configuration Screen**. The main configuration screen will show the current status of your Switch by clicking the model name on top of the function tree.

At the upper right corner of the screen the username and current IP address will be displayed.

Under the username is the **Logout** button. Click this to end this session.

**NOTE:** If you close the web browser without clicking the **Logout** button first, then it will be seen as an abnormal exit and the login session will still be occupied.

Finally, by clicking on the D-Link logo at the upper-left corner of the screen you will be redirected to the local D-Link website.

## *Tool Bar > Save Menu*

The Save Menu provides Save Configuration and Save Log functions.

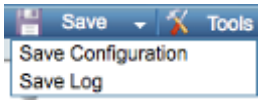


**Figure 28 – Save Menu**

### Save Configuration

Select to save the entire configuration changes you have made to the device to switch's non-volatile RAM.

**Figure 29 – Save Configuration**

### Save Log

Save the log entries to your local drive and a pop-up message will prompt you for the file path. You can view or edit the log file by using text editor (e.g. Notepad).

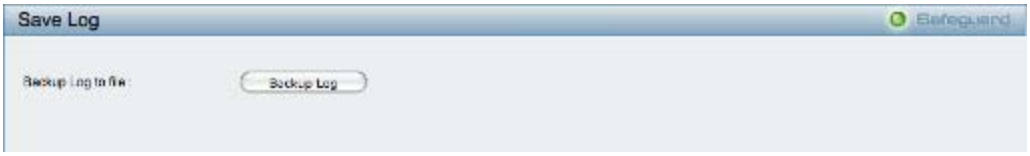


**Figure 30 – Save Log**

## *Tool Bar > Tool Menu*

The Tool Menu offers global function controls such as Reset, Reset System, Reboot Device, Configuration Backup and Restore, Firmware Backup and Upgrade.

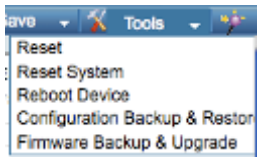


**Figure 31 – Tool Menu**

### Reset

Provide a safe reset option for the Switch. All configuration settings in non-volatile RAM will be reset to factory default except for the IP address.

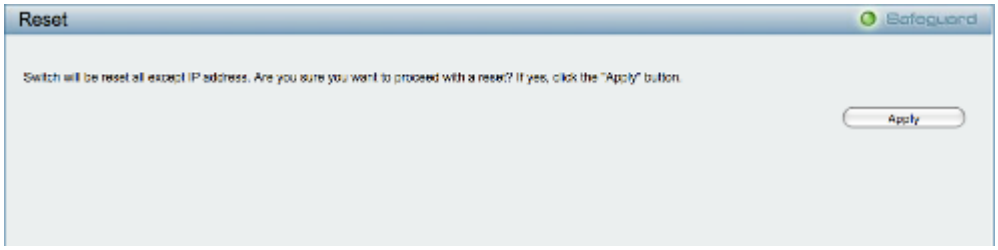
Reset
Safeguard
Switch will be reset all except IP address. Are you sure you want to proceed with a reset? If yes, click the "Apply" button.
Apply

**Figure 32 – Tool Menu > Reset**

### Reset System

Provide another safe reset option for the Switch. All configuration settings in non-volatile RAM will reset to factory default and the Switch will reboot.

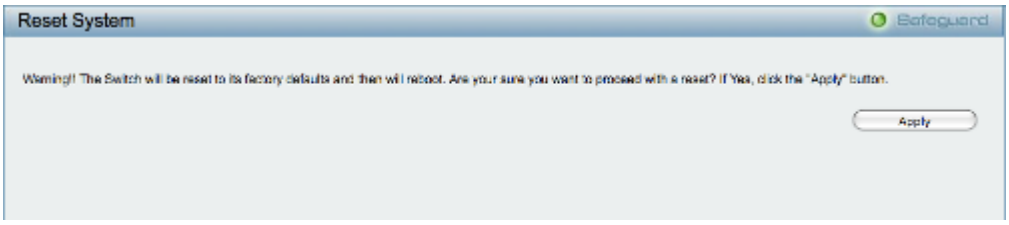
Reset System
Safeguard
Warning! The Switch will be reset to its factory defaults and then will reboot. Are your sure you want to proceed with a reset? If Yes, click the "Apply" button.
Apply

**Figure 33 – Tool Menu > Reset System**

## Reboot Device

Provide a safe way to reboot the system. Click **Reboot** to restart the switch.

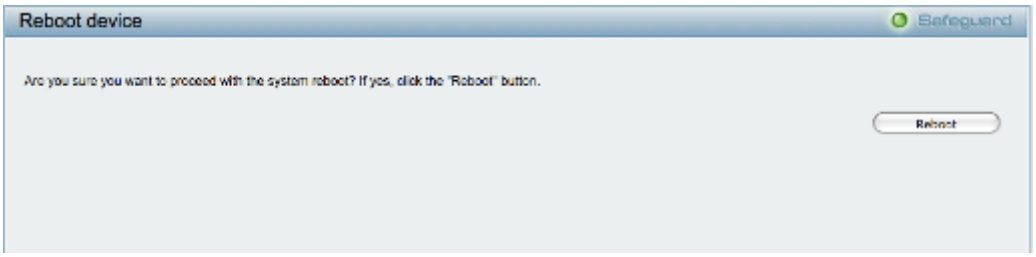


**Figure 34 – Tool Menu > Reboot Device**

## Configuration Backup & Restore

Allow the current configuration settings to be saved to a file (not including the password), and if necessary, you can restore configuration settings from this file. Two methods can be selected: **HTTP** or **TFTP**.

**Figure 35 – Tool Menu > Configure Backup and Restore**

**HTTP:** Backup or restore the configuration file to or from your local drive.

Click **Backup** to save the current settings to your disk.

Click **Browse** to browse your inventories for a saved backup settings file.

Click **Restore** after selecting the backup settings file you want to restore.

**TFTP:** TFTP (Trivial File Transfer Protocol) is a file transfer protocol that allows you to transfer files from/to a remote TFTP server. Specify **TFTP Server IP Address** and **File Name** for the configuration file you want to save to / restore from.

Click **Backup** to save the current settings to the TFTP server.

Click **Restore** after selecting the backup settings file you want to restore.

**Note:** Switch will reboot after restore, and all current configurations will be lost

## Firmware Backup and Upload

Allow for the firmware to be saved, or for an existing firmware file to be uploaded to the Switch. Two methods can be selected: **HTTP** or **TFTP**.

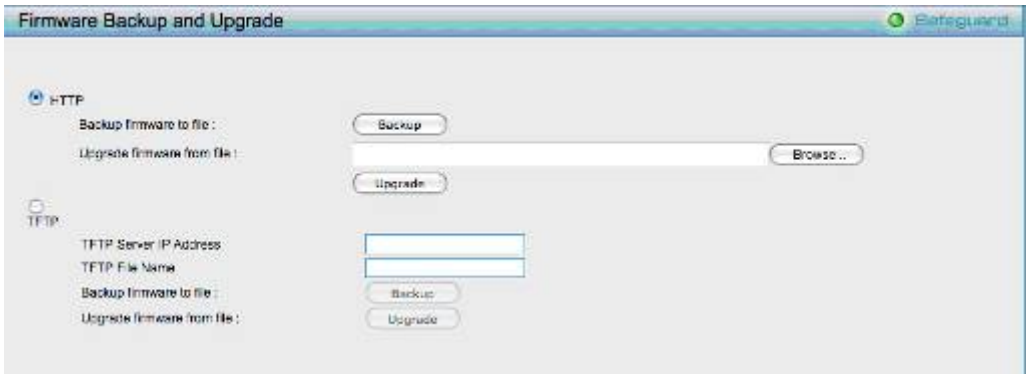


**Figure 36 – Tool Menu > Firmware Backup and Upload**

**HTTP:** Backup or upgrade the firmware to or from your local PC drive.

Click **Backup** to save the firmware to your disk.

Click **Browse** to browse your inventories for a saved firmware file.

Click **Upgrade** after selecting the firmware file you want to restore.

**TFTP:** Backup or upgrade the firmware to or from a remote TFTP server. Specify **TFTP Server IP Address** and **File Name** for the configuration file you want to save to / restore from.

Click **Backup** to save the firmware to the TFTP server.

Click **Upgrade** after selecting the firmware file you want to restore.

**CAUTION:** Do not disconnect the PC or remove the power cord from device until the upgrade completes. The Switch may crash if the Firmware upgrade is incomplete.

### *Tool Bar > Smart Wizard*

By clicking the Smart Wizard button, you can return to the Smart Wizard if you wish to make any changes there.

### *Tool Bar > Online Help*

The Online Help provides two ways of online support: **Online Support Site** will lead you to the D-Link website where you can find online resources such as updated firmware images; **User Guide** can offer an immediate reference for the feature definition or configuration guide.

Online Help
Safeguard
Online Support Site
Please click "Apply" to go to the D-Link online support site at www.dlink.com.
User Guide
Please click "Apply" button to open a window and display the guide in PDF format.

**Figure 37 – Online Help**

Online Help
Safeguard
Online Support Site
Please click "Apply" to go to the D-Link online support site at www.dlink.com.
User Guide
Please click "Apply" button to open a window and display the guide in PDF format.

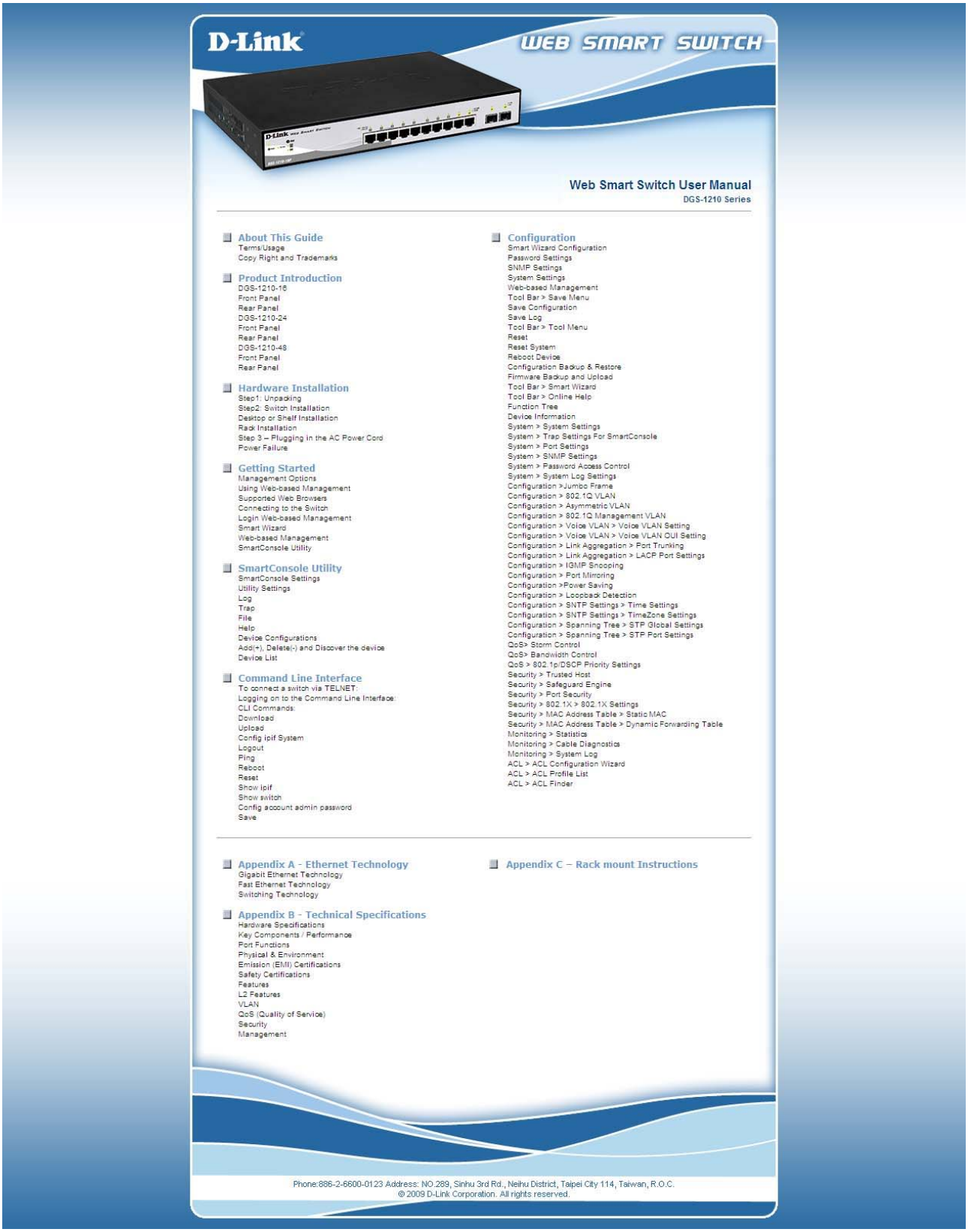


**Figure 38 – User Guide Micro Site**

## *Function Tree*

All configuration options on the switch are accessed through the Setup menu on the left side of the screen. Click on the setup item that you want to configure. The following sections provide more detailed description of each feature and function.

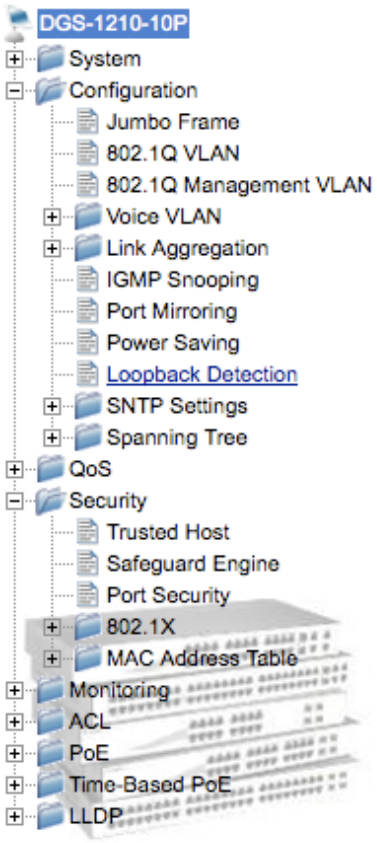


**Figure 39 –Function Tree**

### Device Information

The Device Information provides an overview of the switch, including essential information such as firmware & hardware information, and IP address.

It also offers an overall status of common software features:

**RSTP:** Click **Setting** to link to Configuration > Spanning Tree > STP Global Settings. Default is disabled.

**Port Mirroring:** Click **Setting** to link to Configuration > Port Mirroring. Default is disabled.

**Storm Control:** Click **Setting** to link to Configuration > QoS > Storm Control. Default is disabled.

**Safeguard Engine:** Click **Setting** to link to Configuration > Security > Safeguard Engine. Default is enabled.

**IGMP Snooping:** Click **Setting** to link to Configuration > IGMP Snooping. Default is disabled.

**SNMP:** Click **Setting** to link to System > SNMP Setting. Default is disabled.

**802.1X:** Click **Setting** to link to Configuration > Security > 802.1X > 802.1X Settings. Default is disabled.

**802.1Q Management VLAN:** Click **Setting** to link to Configuration > 802.1Q Management VLAN. Default is disabled.

**DHCP Client:** Click **Setting** to link to System > System Setting. Default is disabled.

**Figure 40 – Device Information**

## System > System Settings

The System Setting allows the user to configure the IP address and the basic system information of the Switch.

**IP Information:** There are two ways for the switch to obtain an IP address: Static and DHCP (Dynamic Host Configuration Protocol).

When using static mode, the **IP Address**, **Subnet Mask** and **Gateway** can be manually configured. When using DHCP mode, the Switch will first look for a DHCP server to provide it with an IP address (including network mask and default gateway) before using the default or previously entered settings. By default the IP setting is static mode with IP address is **10.90.90.90** and subnet mask is **255.0.0.0**.

**System Information:** By entering a **System Name** and **System Location**, the device can more easily be recognized through the SmartConsole Utility and from other Web-Smart devices on the LAN.

**Login Timeout:** The Login Timeout controls the idle time-out period for security purposes, and when there is no action for a specific time span in the Web-based Management. If the current session times out (expires), the user is required a re-login before using the Web-based Management again. Selective range is from 3 to 30 minutes, and the default setting is 5 minutes.

**Group Interval:** The D-Link Web Smart Switch will routinely send report packets to the SmartConsole Utility in order to maintain the information integrity. The user can adjust the **Group Interval** to optimal frequency. Selective range is from 120 to 1225 seconds, and 0 means disabling the reporting function.

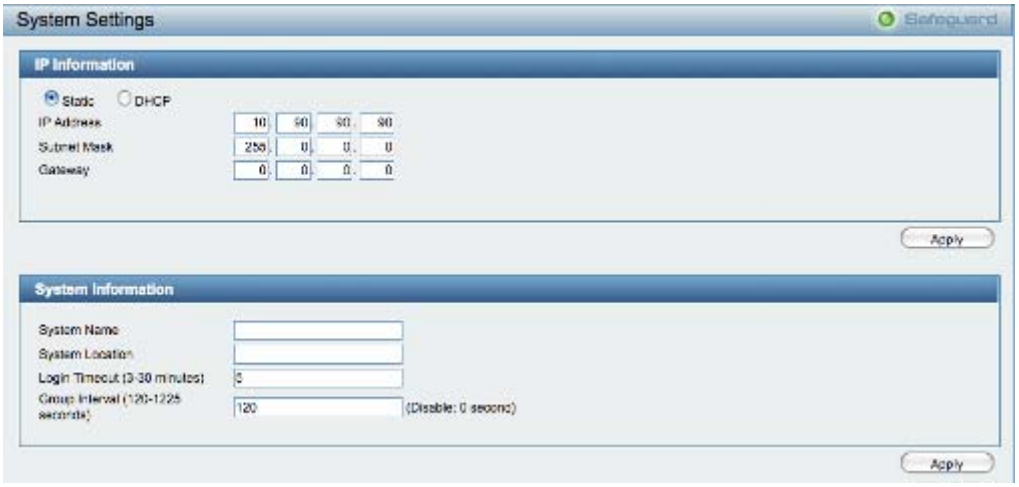


**Figure 41 – System > System Setting**

**System > Trap Settings For SmartConsole**

By configuring the Trap Setting, it allows SmartConsole Utility to monitor specified events on this Web-Smart Switch. By default, Trap Setting is disabled. When the Trap Setting is enabled, enter the **Destination IP** address of the managing station that will receive trap information.

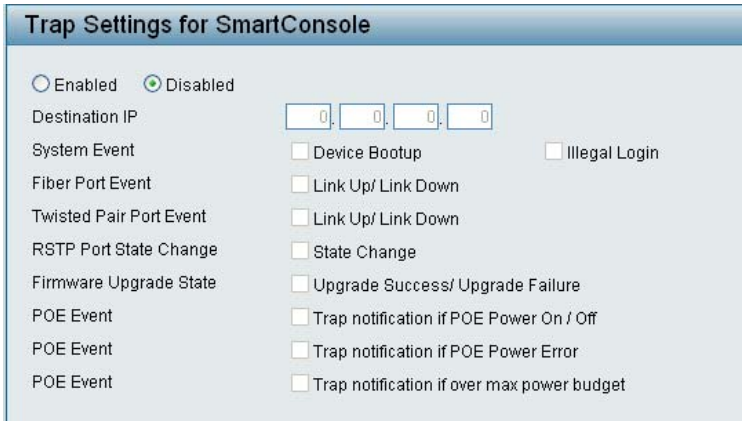


**Figure 42 – System > Trap Setting**

You can select which event message(s) will be sent to the managing station

**System Event:** The system level messages, which contains:

**Device Bootup -** System boot-up information.

**Illegal Login -** Events of incorrect password logins, recording the IP of the originating PC.

**Fiber Port Link Up/Link Down:** Fiber port connection information.

**Twisted pair Port Link Up/Link Down:** Copper port connection information.

**RSTP Port State Change:** Events of a RSTP port state changes.

**Firmware Upgrade State:** Information of firmware upgrade success or failure.

**PoE Power On / Off Event:** PoE port powering information.

**PoE Power Error Event:** Information about PoE powering error.

**PoE over max power budget Event:** over max system power budget information.

**System > Port Settings**

In the Port Setting page, the status of all ports can be monitored and adjusted for optimum configuration. By selecting a range of ports (**From Port** and **To Port**), the **Speed** can be set for all selected ports by clicking **Apply**. Press the **Refresh** button to view the latest information.

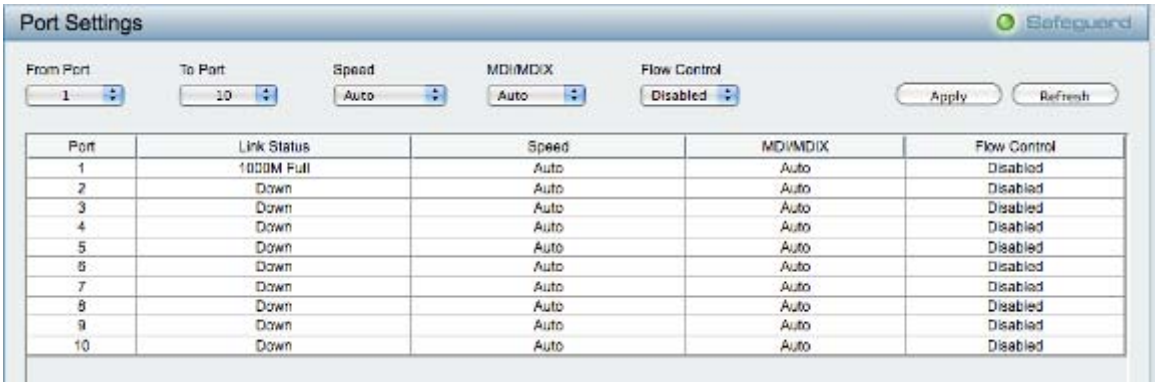


**Figure 43 – System > Port Setting**

**Speed:** Gigabit Fiber connections can operate in 1000M Full Force Mode, Auto Mode or Disabled. Copper connections can operate in Forced Mode settings (1000M Full, 100M Full, 100M Half, 10M Full, 10M Half), Auto, or Disabled. 100M Fiber connections support 100M Full Force Mode, 100M Half Force Mode, or Disabled. The default setting for all ports is **Auto**.

**NOTE:** Be sure to adjust port speed settings appropriately after changing the connected cable

media types.

**MDI/MDIX:**

A **medium dependent interface** (**MDI**) port is an Ethernet port connection typically used on the Network Interface Card (NIC) or Integrated NIC port on a PC. Switches and hubs usually use **Medium dependent interface crossover (MDIX)** interface. When connecting the Switch to end stations, user have to use straight through Ethernet cables to make sure the Tx/Rx pairs match up properly. When connecting the Switch to other networking devices, a crossover cable must be used.

This switch provides a configurable **MDI/MDIX** function for users. The switches can be set as an MDI port in order to connect to other hubs or switches without an Ethernet crossover cable.

**Auto MDI/MDIX** is designed on the switch to detect if the connection is backwards, and automatically chooses MDI or MDIX to properly match the connection. The default setting is "**Auto" MDI/MDIX**.

**Flow Control:** You can enable this function to mitigate the traffic congestion. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control. The default setting is Disabled.

**Link Status:** Reporting **Down** indicates the port is disconnected.

**System > SNMP Settings**

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch or LAN.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The default SNMP setting is disabled. Click **Enabled** to set Community Settings and then **Apply**.

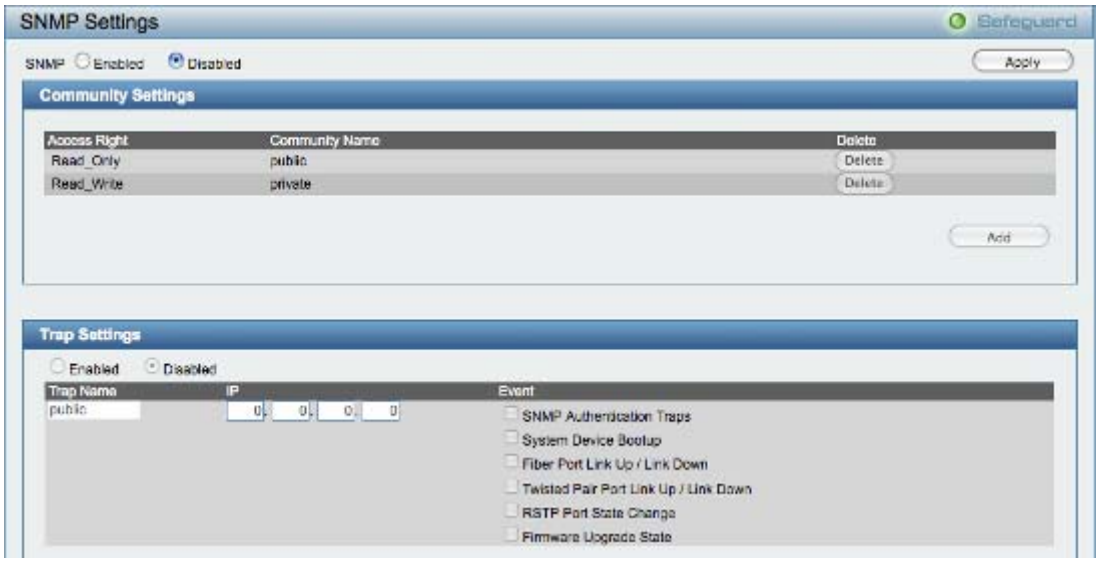


**Figure 44 – System > SNMP Setting**

**Community Setting:** In support of SNMP version 1, the Web-Smart Switch accomplishes user authentication by using Community Settings that function as passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from a station that are not authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 management access are:

**Read_Only:** The community with read-only privilege allows authorized management stations to retrieve MIB objects. The default name is **public**.

**Read_Write:** The community with read/write privilege allows authorized management stations to retrieve and modify MIB objects. The default name is **private**.

**Trap Setting:** Traps are messages that alert network personnel of events that occur on the Switch. Such events can be as severe as a reboot (someone accidentally turned the Switch OFF), or less serious events such as a port status change. The Switch can generate traps and send them to the trap recipient (i.e. network administrator).

**Setting up a Trap:** Select **Enable**, enter a Trap Name, add the IP of the device to be monitored, and select the event(s) to trap. The available trap Events to choose from include:

- SNMP Authentication Traps
- System Device Bootup
- Fiber Link Up / Link Down
- Twisted Pair Link Up / Link Down
- RSTP Port State Change
- Firmware Upgrade State
- Trap notification if POE Power On / Off
- Trap notification if POE Power Error
- Trap notification if over max power budget

**Note:** Trap Name must be selected from a Community Name

## System > Password Access Control

Setting a password is a critical tool for managers to secure the Web-Smart Switch. After entering the old password and the new password twice, click **Apply** for the changes to take effect.

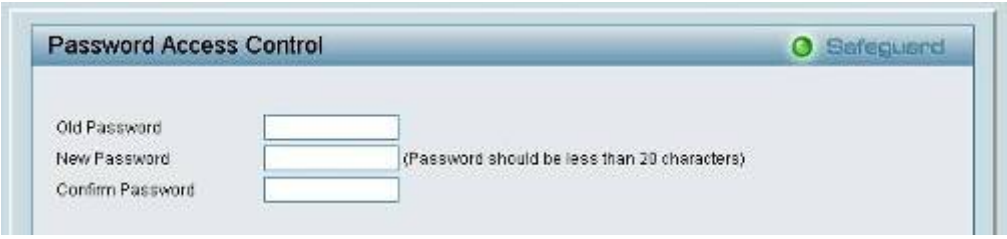


**Figure 45 – System > Password Access Control**

## System > System Log Settings

System Logs record and manage events, as well as report errors and informational messages. Message severity determines a set of event messages that will be sent. Click **Enable** so you can start to configure the related settings of the remote system log server, then press **Apply** for the changes to take effect.

**Figure 46 – System > System Log Settings**

**Server IP Address:** Specifies the IP address of the system log server.

**UDP Port:** Specifies the UDP port to which the server logs are sent. The possible range is 1 – 65535, and the default value is 514.

**Time Stamp**: Select Enable to time stamp log messages.

**Severity:** Specifies the minimum severity from which warning messages are sent to the server. There are three levels. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible levels are:

**Warning -** The lowest level of a device warning. The device is functioning, but an operational problem has occurred.

**Informational -** Provides device information.

**All -** Displays all levels of system logs.

**Facility:** Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 ~ Local 7),

## Configuration > Jumbo Frame

D-Link Gigabit Web Smart Switches support jumbo frames (frames larger than the Ethernet frame size of 1536 bytes) of up to 10,000 bytes (tagged). Default is disabled, Select **Enabled** then click **Apply** to turn on the jumbo frame support.

6

**Figure 47 – Configuration > Jumbo Frame**

## Configuration > 802.1Q VLAN

A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area.

VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections.

The IEEE 802.1Q VLAN Configuration page provides powerful VID management functions. The original settings have the VID as 1, no default name, and all ports as “Untagged”

**Rename:** Click to rename the VLAN group.

**Delete VID:** Click to delete the VLAN group.

**Add New VID:** Click to create a new VID group, assigning ports from 01 to 10 as **Untag**, **Tag**, or **Not Member**. A port can be untagged in only one VID. To save the VID group, click **Apply.**

You may change the name accordingly to the desired groups, such as R&D, Marketing, email, etc.

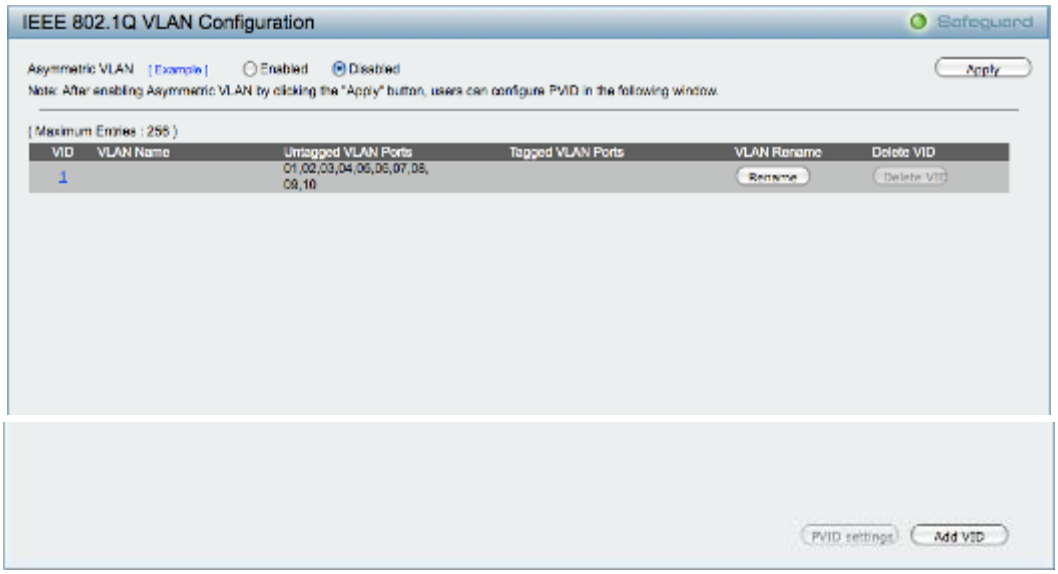

**Figure 48 – Configuration > 802.1Q VLAN > Default Setting**

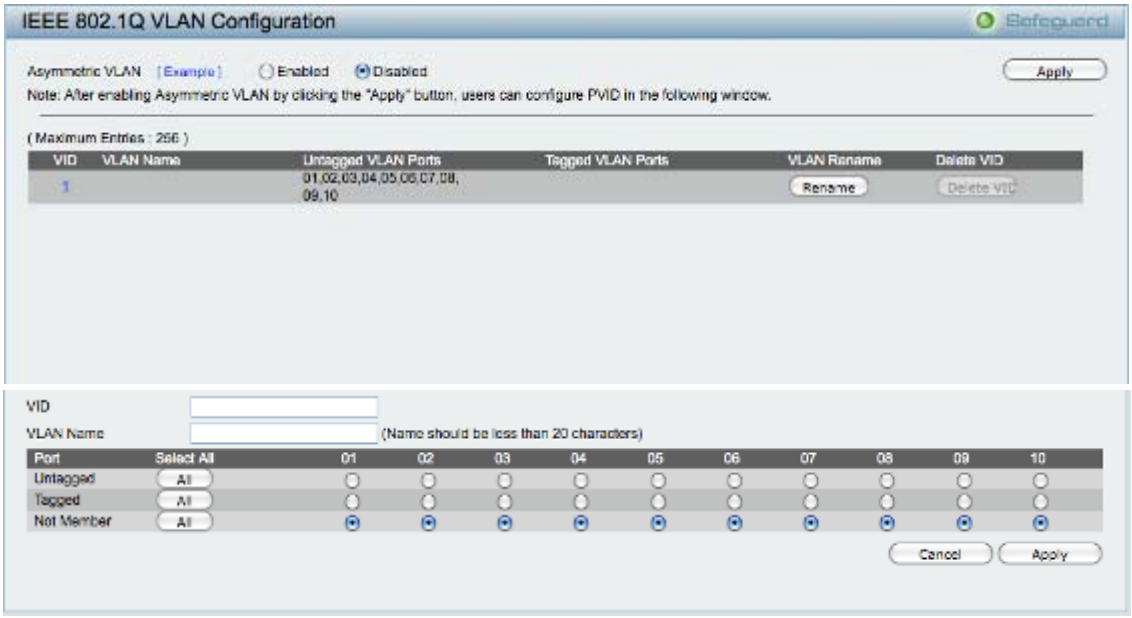
IEEE 802.1Q VLAN Configuration
Safeguard
Asymmetric VLAN [Example] Enabled Disabled
Apply
Note: After enabling Asymmetric VLAN by clicking the "Apply" button, users can configure PVID in the following window.
( Maximum Entries : 256 )
VID VLAN Name Untagged VLAN Ports Tagged VLAN Ports VLAN Rename Delete VID
1 01,02,03,04,05,06,07,08, 09,10 Rename Delete VID
VID
VLAN Name
(Name should be less than 20 characters)
Port Select All 01 02 03 04 05 06 07 08 09 10
Untagged All
Tagged All
Not Member All
Cancel
Apply

**Figure 49 – Configuration > 802.1Q VLAN > Add VID**

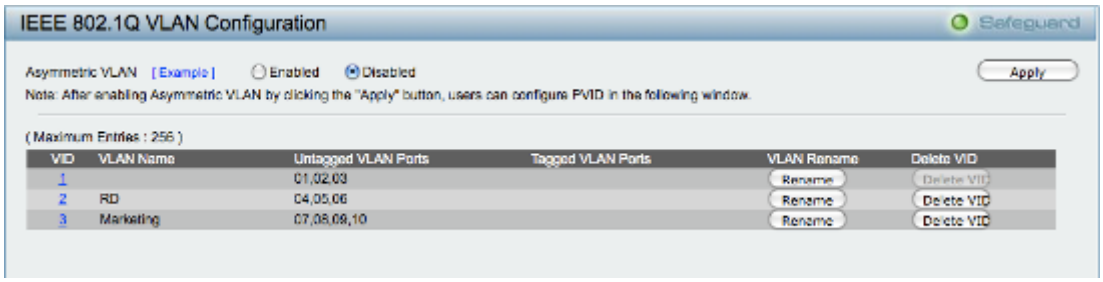
IEEE 802.1Q VLAN Configuration
Safeguard
Asymmetric VLAN [Example] Enabled Disabled
Apply
Note: After enabling Asymmetric VLAN by clicking the "Apply" button, users can configure PVID in the following window.
( Maximum Entries : 256 )
VID VLAN Name Untagged VLAN Ports Tagged VLAN Ports VLAN Rename Delete VID
1 01,02,03 Rename Delete VID
2 RD 04,05,06 Rename Delete VID
3 Marketing 07,08,09,10 Rename Delete VID

**Figure 50 – Configuration > 802.1Q VLAN > Example VIDs**

**Figure 51 – Configuration > 802.1Q VLAN > VID Assignments**

## Configuration > Asymmetric VLAN

This function is located in the 802.1Q Configuration page. It allows devices in different VLANs to communicate with the servers, firewalls or other shared resources in the shared VLAN. This configuration is accomplished in three steps:

- Enabling Asymmetric VLAN function
- Creating shared VLAN and access VLAN
- Configuring the PVID of access VLAN

Asymmetric VLAN is especially effective when used in a small network where a L3 routing device is absent, or if the resource to be shared is not capable of supporting tagged VLAN (for example, a printer).

The example below is a typical application of Asymmetric VLAN. Servers and firewall are located in shared VLAN (default VLAN), and PCs 1, 2 and 3 are located in different VLAN. Because VLANs remain separate,

PCs 1, 2, and 3 cannot communicate with each other; but all of them need to access the servers or the Internet behind the firewall.

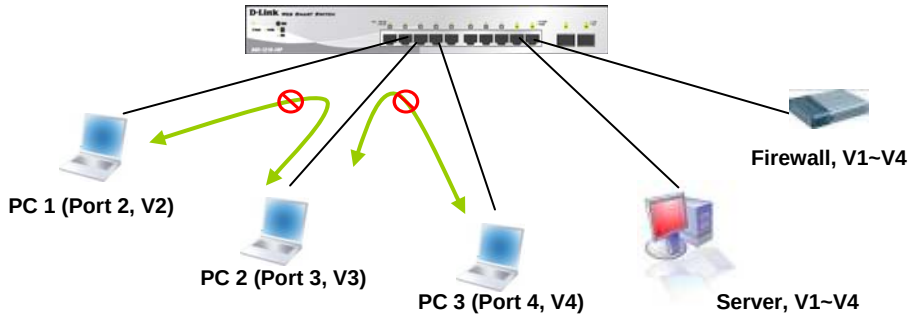


**Figure 52 – Configuration > 802.1Q VLAN > Asymmetric VLAN Example**

1. Enable Asymmetric VLAN

Enable Asymmetric VLAN and click the **Apply** button. The overlapping VLAN cannot be configured unless this function is enabled..

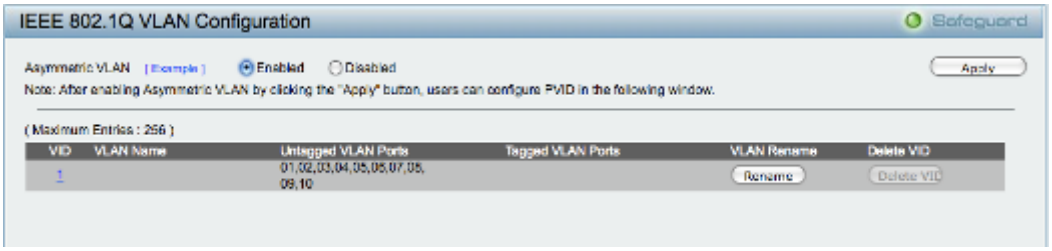


**Figure 53 – Configuration > 802.1Q VLAN > Asymmetric VLAN - Enabling Asymmetric VLAN**

**2. Configure the shared VLAN (VLAN 1) and access VLANs (VLAN 2, 3, 4)**

In this case, the default VLAN is used as shared VLAN, and the ports that are shared in the network are:

- Port 9 is connected to the server
- Port 10 is connected to the firewall

The group of shared ports needs to be included for all the VLANs. Ports 9, 10 already belong to VLAN 1, therefore no changes are needed.

VLAN 2 is configured to include ports 9, 10 (shared VLAN ports) and the set of ports to be separated from the other VLANs (for example, port 2). VLAN 3 and 4 are then configured to include shared ports and the set of ports to be separated from the other VLANs (for example, port 3 and 4 respectively). Therefore we have three VLANs that share some common ports, but their original membership ports are still separated from each other (for example, port 2, 3, and 4).

The VLAN settings of this example are:

- VLAN 1: default VLAN 1, including all ports with untagged.
- VLAN 2: Member ports are untagged port 2, 9, 10.
- VLAN 3: Member ports are untagged port 3, 9, 10.
- VLAN 4: Member ports are untagged port 4, 9, 10.

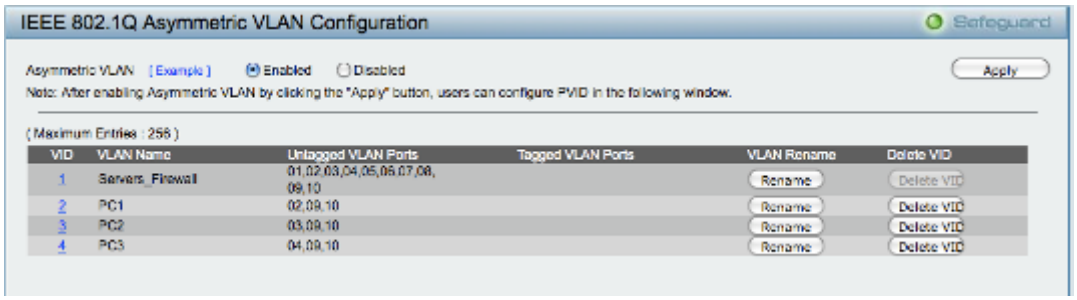
IEEE 802.1Q Asymmetric VLAN Configuration
Safeguard
Asymmetric VLAN [ Example ] Enabled Disabled
Apply
Note: After enabling Asymmetric VLAN by clicking the "Apply" button, users can configure PVID in the following window.
( Maximum Entries : 256 )
VID VLAN Name Untagged VLAN Ports Tagged VLAN Ports VLAN Rename Delete VID
1 Servers_Firewall 01,02,03,04,05,06,07,08, 09,10 Rename Delete VID
2 PC1 02,09,10 Rename Delete VID
3 PC2 03,09,10 Rename Delete VID
4 PC3 04,09,10 Rename Delete VID

**Figure 54 – Configuration > 802.1Q VLAN > Asymmetric VLAN – Create VLANs**

### 3. Configuring the PVID of access VLAN

Configure the PVID setting located at the bottom of the VLAN configuration page. The user needs to set the shared set of ports as PVID 1, and the other separated groups of ports (for example, port 2, 3, and 4) as PVID 2, 3 and 4 respectively.

The purpose of assigning PVID is to make sure the untagged packets will be transmitted correctly.

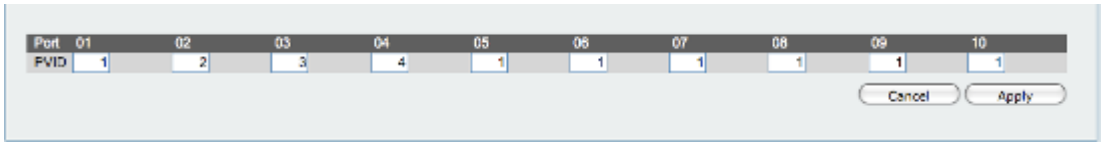


**Figure 55 – Configuration > 802.1Q VLAN > Asymmetric VLAN – Assign PVID**

After configuration, the user will be able to share the network resources set on the shared group of ports (nominated as PVID 1), with both smaller subsets of VLANs (nominated PVID 2, 3 and 4). However, VLAN 2, 3 and 4 groups are incapable of sharing information with each other directly. Click **Example** to see the example to configure asymmetric VLAN in larger networks.

**Note:** When Asymmetric VLAN is enabled, IGMP Snooping, Management VLAN, and MAC address table will be reset to default.

## Configuration > 802.1Q Management VLAN

The 802.1Q Management VLAN setting allows you to transfer the authority of the switch from the default VLAN to others created by users. This allows managing the whole network more flexible.

By default, the Management VLAN is disabled. You can select any existing VLAN as the management VLAN when this function is enabled. There can only be one management VLAN at a time.

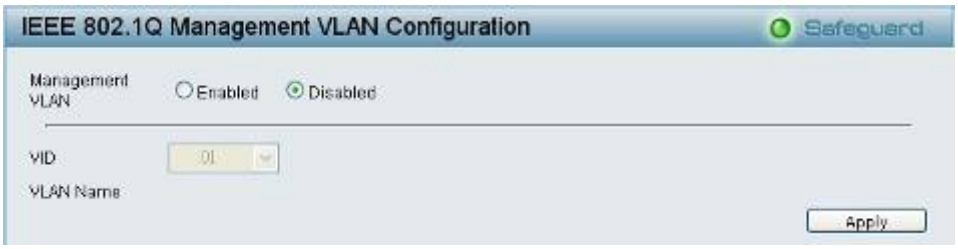


**Figure 56 – Configuration > 802.1Q Management VLAN**

## Configuration > Voice VLAN > Voice VLAN Setting

Voice VLAN is a feature that allows you to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of VoIP traffic are guaranteed. The Voice VLAN function will only insert the Voice VLAN tag to untagged packets under corresponding ports. If a VoIP packet comes with a VLAN tag, the Voice VLAN function won't replace the original VLAN tag.

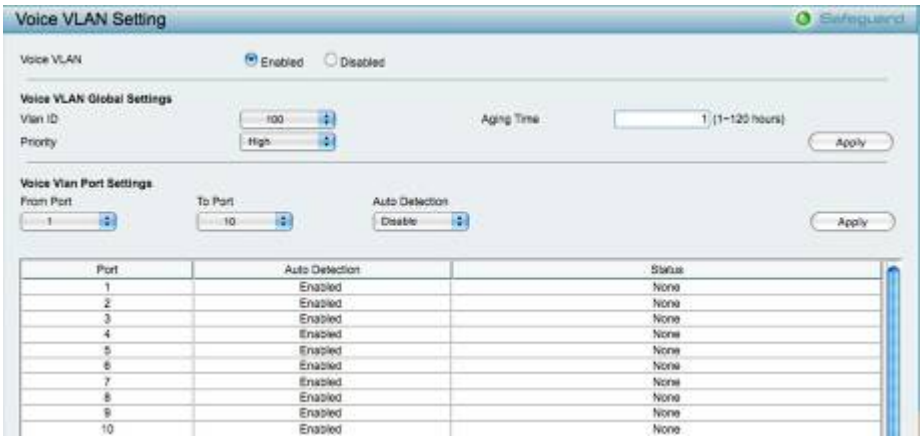


**Figure 57 – Configuration > Voice VLAN > Voice VLAN Setting**

**Voice VLAN State:** Select to enable or disable Voice VLAN. The default is *Disabled.* After you enabled Voice VLAN, you can configure the **Voice VLAN Global Settings**.

**VLAN ID:** The ID of VLAN that you want to assign voice traffic to. You must first create a VLAN from the 802.1Q VLAN page before you can assign a dedicated Voice VLAN. The member port you configured in 802.1Q VLAN setting page will be the static member port of voice VLAN. To dynamically add ports into the voice VLAN, please enable the **Auto Detection** function

**Priority:** The 802.1p priority levels of the traffic in the Voice VLAN.

**Aging Time:** Enter a period of time (in hours) to remove a port from the voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will start. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. Selectable range is from 1 to 120 hours, and default is 1 hour.

**From Port / To Port:** A consecutive group of ports may be configured starting with the selected port.

**Auto Detection:** Switch will add ports to the voice VLAN automatically if it detects the device OUI matches the Telephony OUI configured in the Voice VLAN OUI Setting page. Use the drop-down menu to enable or disable the OUI auto detection function. The default is *Disabled*

Click **Apply** to implement changes made.

**Note:** Voice VLAN has higher priority than any other features (including QoS). Therefore the voice traffic will be operated according to the Voice VLAN setting and not impacted by the QoS feature.

## Configuration > Voice VLAN > Voice VLAN OUI Setting

This window allows the user to configure the user-defined voice traffic's OUI. An Organizationally Unique Identifier (OUI) is the first three bytes of the MAC address. This identifier uniquely identifies a vendor, manufacturer, or other organization.

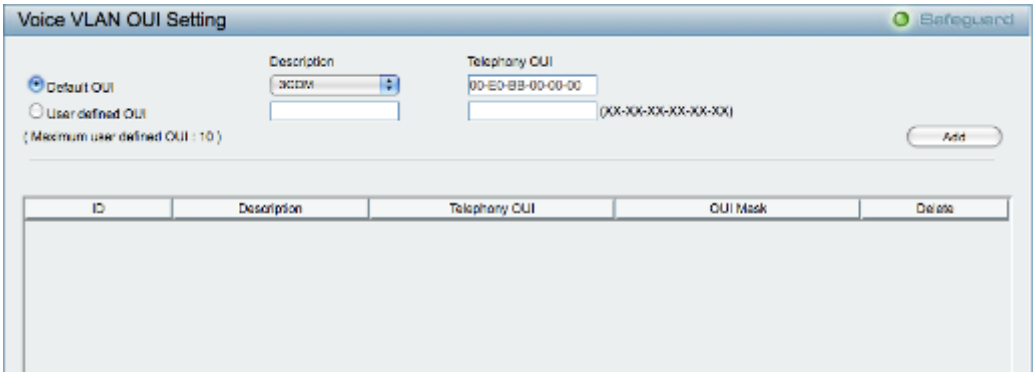


**Figure 58 – Configuration > Voice VLAN > Voice VLAN OUI Setting**

There are some pre-defined OUIs and when the user configures personal OUI, these pre-defined OUIs must be avoided. Below are the pre-defined voice traffic's OUI:

| OUI | Vendor | Mnemonic Name |
|---|---|---|
| 00:E0:BB | 3Com | 3com |
| 00:03:6B | Cisco | cisco |
| 00:E0:75 | Veritel | veritel |
| 00:D0:1E | Pingtel | pingtel |
| 00:01:E3 | Siemens | siemens |
| 00:60:B9 | NEC/ Philips | nec&philips |
| 00:0F:E2 | Huawei-3COM | huawei&3com |
| 00:09:6E | Avaya | avaya |

**Default OUI:** Pre-defined OUI values, including brand names of 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei3COM, and Avaya.

**User defined OUI:** You can manually create a Telephony OUI with a description. The maximum number of user defined OUIs is 10. It will occupy one ACL rule when selecting a user defined OUI by default, and to configure one user-defined OUI will take extra one ACL rule. System will auto generate an ACL profile (Profile ID: 51) for all the Voice VLAN rules.

Select the OUI and press **Add** to the lower table to complete the Auto Voice VLAN setting.

**Configuration > Link Aggregation > Port Trunking**

The Trunking function enables the combining of two or more ports together to increase bandwidth. Up to five Trunk groups may be created, and each group consists up to eight ports. Select the ports to be grouped together, and then click **Apply** to activate the selected Trunking groups. Two types of link aggregation can be selected:

**Static -** Static link aggregation.

**LACP -** LACP (Link Aggregation Control Protocol) is enabled on the device. LACP allows for the automatic detection of links in a Port Trunking Group.

**Disable -** Remove all members in this trunk group.

**Figure 59 – Configuration > Link Aggregation > Port Trunking**

**NOTE:** Each combined trunk port must be connected to devices within the same VLAN group.

## Configuration > Link Aggregation > LACP Port Settings

The **LACP Port Settings** is used to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames

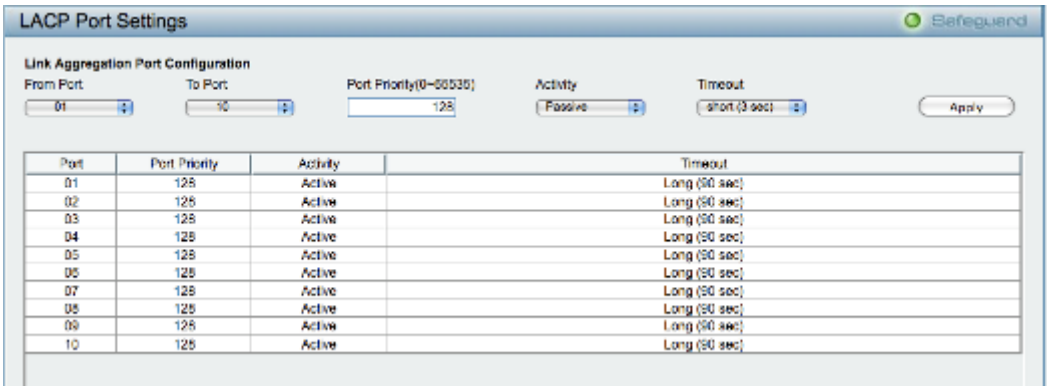


**Figure 60 – Configuration > Link Aggregation > LACP Port Settings**

**From Port:** The beginning of a consecutive group of ports may be configured starting with the selected port.

**To Port:** The ending of a consecutive group of ports may be configured starting with the selected port.

**Port Priority (0-65535):** Displays the LACP priority value for the port. Default is 128.

**Activity:** There are two different roles of LACP ports:

**Active -** Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

**Passive -** LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports.

**Timeout:** Specify the administrative LACP timeout. The possible field values are:

**Short (3 Sec)** - Defines the LACP timeout as 3 seconds.

**Long (90 Sec)** - Defines the LACP timeout as 90 seconds. This is the default value.

Click **Apply** to implement the changes made.

## Configuration > IGMP Snooping

With Internet Group Management Protocol (IGMP) snooping, the Web Smart Switch can make intelligent multicast forwarding decisions by examining the contents of each frame's Layer 2 MAC header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the Web Smart Switch will forward multicast traffic only to connections that have group members attached.

The settings of IGMP snooping is set by each VLAN individually.

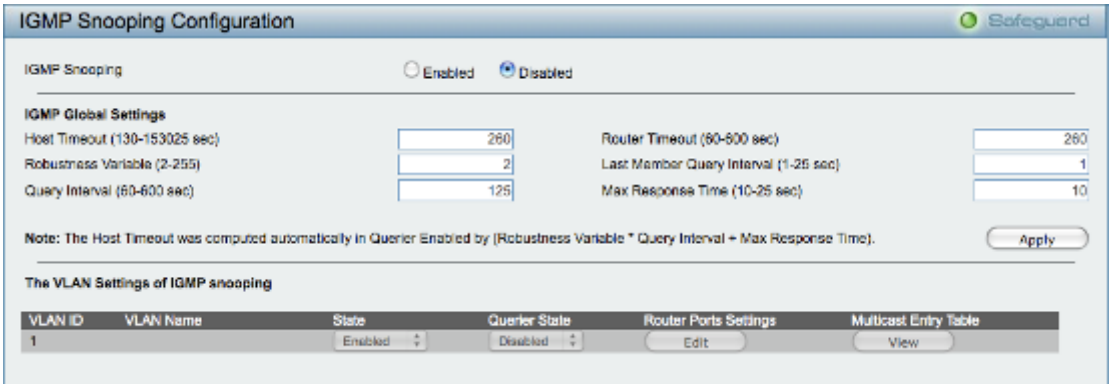

**Figure 61 – Configuration > IGMP Snooping Configuration**

By default, IGMP is disabled. If enabled, the IGMP Global Settings will need to be entered:

**Host Timeout (130-153025 sec):** This is the interval after which a learned host port entry will be purged. For each host port learned, a 'Port Purge Timer' runs for 'Host Port Purge Interval'. This timer will be restarted whenever a report message from host is received over that port. If no report messages are received for 'Host Port Purge Interval' time, the learned host entry will be purged from the multicast group. The default value is 260 seconds.

**Robustness Variable (2-255 sec):** The Robustness Variable allows adjustment for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may need to be increased. The Robustness Variable cannot be set to zero, and it SHOULD NOT be. Default is 2 seconds.

**Query Interval (60-600 sec):** The Query Interval is the interval between General Queries sent. By adjusting the Query Interval, the number of IGMP messages can be increased or decreased; larger values will cause IGMP Queries to be sent less often. Default value is 125 seconds.

**Router Timeout (60-600 sec):** This is the interval after which a learned router port entry will be purged. For each router port learned, a 'Router Port Purge Timer' runs for 'Router Port Purge Interval'. This timer will be restarted whenever a Query control message is received over that port. If there are no Query control messages received for 'Router Port Purge Interval' time, the learned router port entry will be purged. Default is 260 seconds.

**Last Member Query Interval (1-25 sec):** The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group. Default is 1 second.

**Max Response Time (10-25 sec):** The Max Response Time specifies the maximum allowed time before sending a responding report message. Adjusting this setting effects the "leave latency", or the time between the moment the last host leaves a group and when the multicast server is notified that there are no more members. It also allows adjustments for controlling the frequency of IGMP traffic on a subnet. Default is 10 seconds.

**Querier State:** D-Link Smart Switch is able to send out the IGMP Queries to check the status of multicast clients. Default is disabled.

To enable IGMP snooping for a given VLAN, select enable and click on the **Apply** button. Then press the **Edit** button under **Router Port Setting**, and select the ports to be assigned as router ports for IGMP snooping for the VLAN. Press **Apply** for changes to take effect. A router port configured manually is a **Static Router Port**, and a **Dynamic Router Port** is dynamically configured by the Switch when a query control message is received.

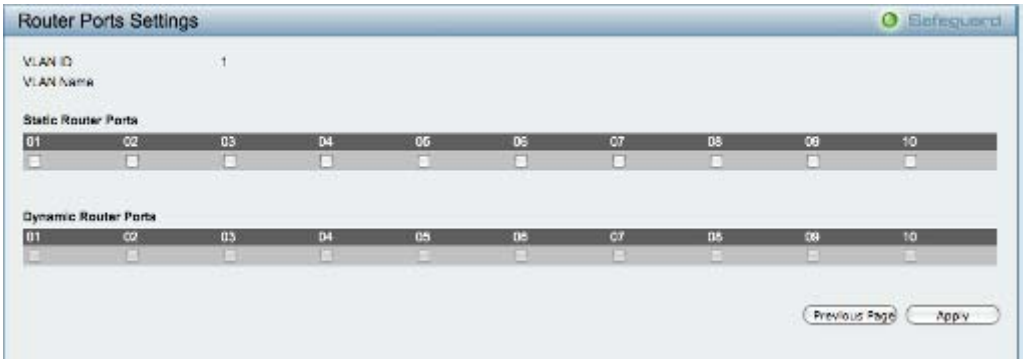


**Figure 62 – Configuration > IGMP Snooping > IGMP Router port Settings**

To view the Multicast Entry Table for a given VLAN, press the **View** button.

**Figure 63 – Configuration > IGMP Multicast Entry Table**

## Configuration > Port Mirroring

Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of the Switch to another port, where the packet can be studied. This enables network managers to better monitor network performances.

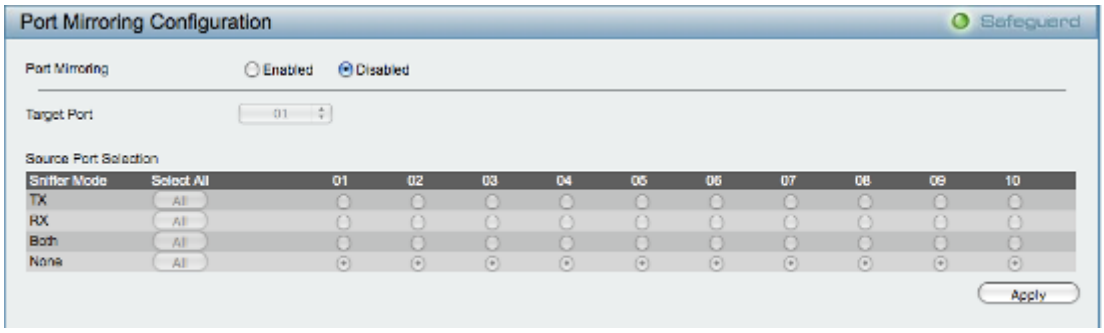


**Figure 64 – Configuration > Port Mirroring**

Selection options for the Source Ports are as follows:

**TX (transmit) mode:** Duplicates the data transmitted from the source port and forwards it to the Target Port. Click “all” to include all ports into port mirroring.

**RX (receive) mode:** Duplicates the data that is received from the source port and forwards it to the Target Port. Click “all” to include all ports into port mirroring.

**Both (transmit and receive) mode:** Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. Click “all” to include all ports into port mirroring.

**None:** Turns off the mirroring of the port. Click “all” to remove all ports from mirroring.

## Configuration > Power Saving

The Power Saving mode feature reduces power consumption automatically when the RJ-45 port is link down or the connected devices are turned off. Less power will be consumed also when the short cable is used (less than 20 meters).

By reducing power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Power Saving mode is enabled. Click **Apply** to make the change effective.

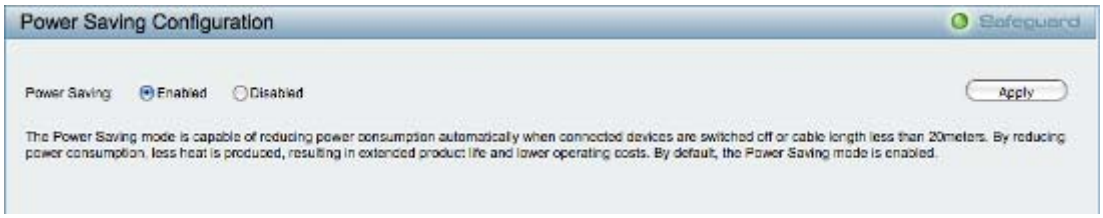
Power Saving Configuration
Safeguard
Power Saving:
Enabled
Disabled
Apply
The Power Saving mode is capable of reducing power consumption automatically when connected devices are switched off or cable length less than 20meters. By reducing power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Power Saving mode is enabled.

**Figure 65 – Configuration > Power Saving**

## Configuration > Loopback Detection

The Loopback Detection function is used to detect the loop created by a specific port while Spanning Tree Protocol (STP) is not enabled in the network, especially when the down links are hubs or unmanaged switches. The Switch will automatically shutdown the port and sends a log to the administrator. The Loopback Detection port will be unlocked when the Loopback Detection **Recover Time** times out. The Loopback Detection function can be implemented on a range of ports at the same time. You may enable or disable this function using the pull-down menu.

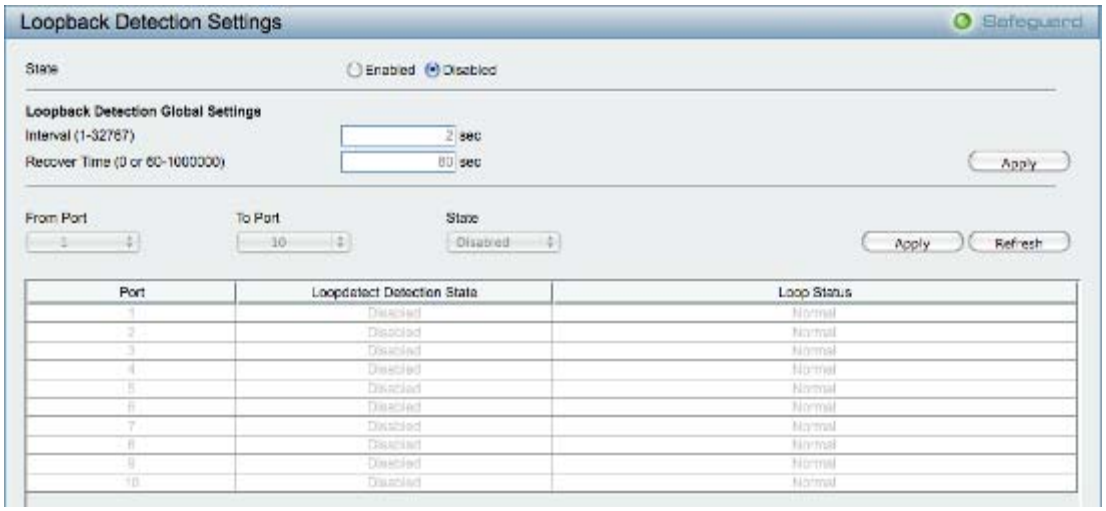


**Figure 66 – Configuration > Loopback Detection**

**Loopback Detection State:** Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*

**Interval (1-32767):** Set a Loop detection Interval between *1* and *32767* seconds. The default is *1* seconds.

**Recover Time (0 or 60-1000000):** Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loop Detection Recover Time. The default is *60* seconds.

**From Port:** The beginning of a consecutive group of ports may be configured starting with the selected port.

**To Port:** The ending of a consecutive group of ports may be configured starting with the selected port.

**State:** Use the drop-down menu to toggle between *Enabled* and *Disabled.* Default is *Disabled*.

Click **Apply** to implement changes made.

**Configuration > SNTP Settings > Time Settings**

SNTP or Simple Network Time Protocol is used by the Switch to synchronize the clock of the computer. The SNTP settings folders contain two windows: Time Settings and TimeZone Settings. Users can configure the time settings for the switch, and the following parameters can be set or are displayed in the Time Settings page.

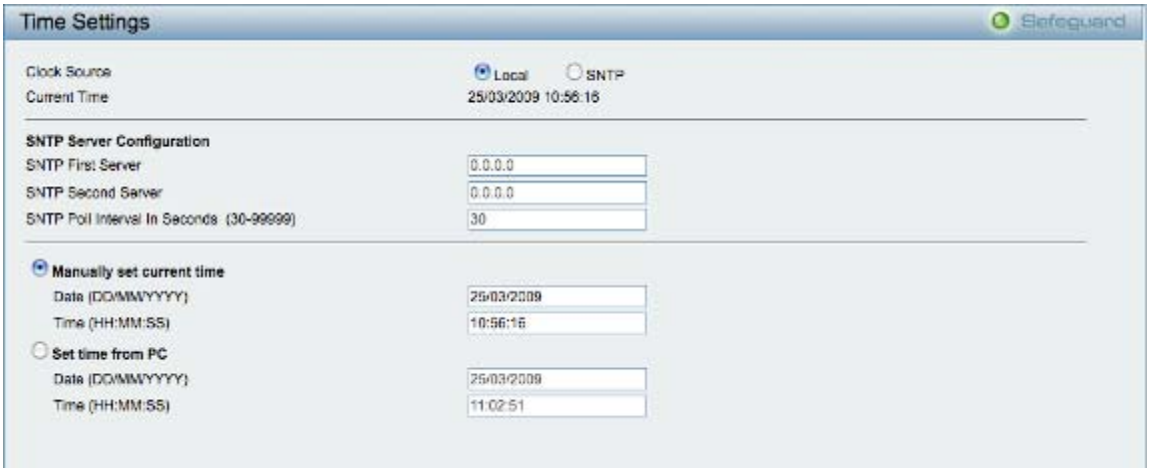


**Figure 67 – Configuration > SNTP Settings > Time Settings**

**Clock Source:** Specify the clock source by which the system time is set. The possible options are:

**Local -** Indicates that the system time is set locally by the device.

**SNTP -** Indicates that the system time is retrieved from a SNTP server.

**Current Time:** Displays the current date and time for the switch.

If choosing **SNTP** for the clock source, then the following parameters will be available:

**SNTP First Server:** Specify the IP address of the primary SNTP server from which the system time is retrieved.

**SNTP Second Server:** Specify the IP address of the secondary SNTP server from which the system time is retrieved.

**SNTP Poll Interval in Seconds (30-99999):** Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 30 seconds.

Click **Apply** to implement changes made.

When selecting **Local** for the clock source, users can select from one of two options:

**Manually set current time:** Users input the system time manually.

**Set time from PC:** The system time will be synchronized from the local computer.

**Configuration > SNTP Settings > TimeZone Settings**

The TimeZone Setting Page is used to configure time zones and Daylight Savings time settings for SNTP.

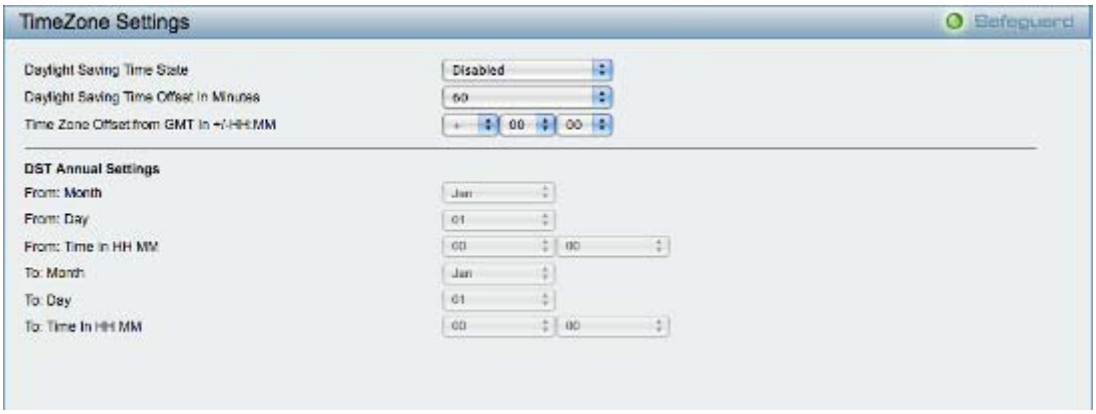


**Figure 68 – Configuration > SNTP Settings > TimeZone Settings**

**Daylight Saving Time State:** Use this drop-down menu to enable or disable the DST Settings.

**Daylight Saving Time Offset in Minutes:** Use this drop-down menu to specify the amount of time that will constitute your local DST offset - *30*, *60*, *90*, or *120* minutes.

**Time Zone Offset from GMT in +/- HH:MM:** Use these drop-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)

**DST Annual Settings:** Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date must not be in the same month. For example, specify to begin DST on March 8 and end DST on November 1.

**From: Month:** Enter the month DST will start on, each year.

**From: Day:** Enter the day of the week DST will start on, each year.

**From: Time in HH:MM:** Enter the time of day DST will start on, each year.

**To: Month:** Enter the month DST will end on, each year.

**To: Day:** Enter the date DST will end on, each year.

**To: Time in HH:MM:** Enter the time of day that DST will end on, each year.

Click **Apply** to implement changes made.

**Configuration > Spanning Tree > STP Global Settings**

The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1D STP. RSTP can operate with legacy equipment implementing IEEE 802.1D, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

By default, Rapid Spanning Tree is disabled. If enabled, the Switch will listen for BPDU packets and its accompanying Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment.

After enabling STP, setting the STP Global Setting includes the following options:

**Figure 69 – Configuration > Spanning Tree > STP Global Settings**

**STP Version:** You can choose RSTP or STP Compatible. The default setting is RSTP.

**Bridge Priority:** This value between 0 and 61410 specifies the priority for forwarding packets: the lower the value, the higher the priority. The default is 32768.

**TX Hold Count (1-10):** Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6.*

**Maximum Age (6-40 sec):** This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that the Switch has the lowest Bridge Identifier, it will become the Root Bridge. A time interval may be chosen between 6 and 40 seconds. The default value is 20. (Max Age has to have a value bigger than Hello Time)

**Hello Time (1-10 sec):** The user may set the time interval between transmissions of configuration messages by the root device, thus stating that the Switch is still functioning. The default is 2 seconds.

**Forward Delay (4-30 sec):** This sets the maximum amount of time that the root device will wait before changing states. The default is 15 seconds.

**Root Bridge:** Displays the MAC address of the Root Bridge.

**Root Maximum Age:** Displays the Maximum Age of the Root Bridge.

**Root Forward Delay:** Displays the Forward Delay of the Root Bridge.

**Root port:** Displays the root port.

Click **Apply** for the settings to take effect. Click **Refresh** to renew the page.

**Configuration > Spanning Tree > STP Port Settings**

STP can be set up on a port per port basis. In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of the groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

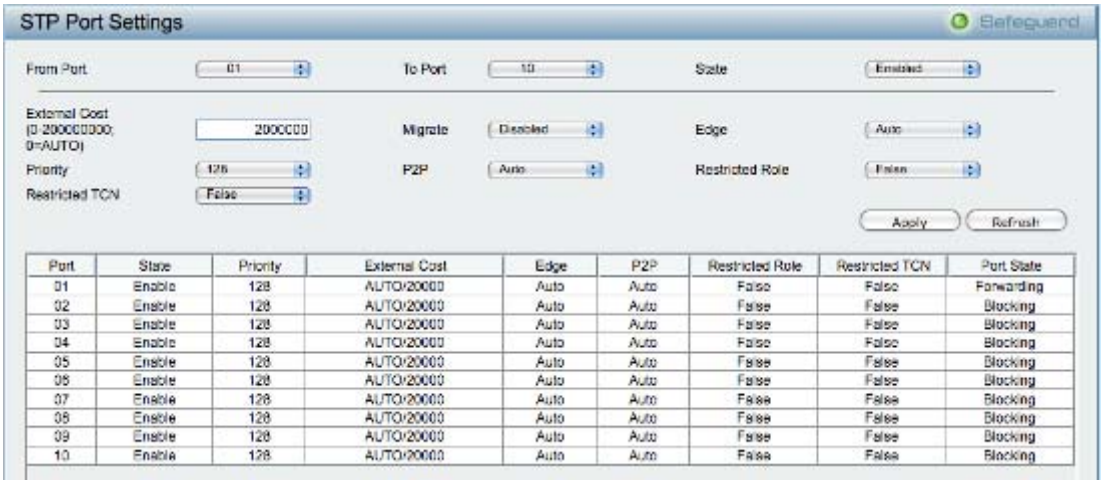
STP Port Settings
Safeguard
From Port
01
To Port
10
State
Enabled
External Cost (0 200000000; 0=AUTO)
2000000
Migrate
Disabled
Edge
Auto
Priority
128
P2P
Auto
Restricted Role
False
Restricted TCN
False
Apply
Refresh
Port | State | Priority | External Cost | Edge | P2P | Restricted Role | Restricted TCN | Port State
01 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Forwarding
02 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking
03 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking
04 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking
05 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking
06 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking
07 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking
08 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking
09 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking
10 | Enable | 128 | AUTO/20000 | Auto | Auto | False | False | Blocking

**Figure 70 – Configuration > Spanning Tree > STP Port Settings**

**From Port/To Port:** A consecutive group of ports may be configured starting with the selected port.

**State:** Use the drop-down menu to enable or disable STP by per-port based. It will be selectable after the global STP is enabled.

**External Cost:** This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto).

> **0 (auto) -** Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.
>
> **Value 1-200000000 -** Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

**Migrate:** Setting this parameter as *Yes* will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.

**Edge:** Selecting the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Selecting the *False* parameter indicates that the port does not have edge port status. Selecting the *Auto* parameter indicates that the port have edge port status or not have edge port status automatically.

**Priority:** Specify the priority of each port. Selectable range is from 0 to 240, and the default setting is 128. The lower the number, the greater the probability the port will be chosen as a root port.

**P2P:** Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex.

Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *False*. The default setting for this parameter is *Auto*.

**Restricted Role:** Toggle between *True* and *False* to set the restricted role state of the packet. If set to *True*, the port will never be selected to be the Root port. The default value is *False*.

**Restricted TCN:** Toggle between *True* and *False* to set the restricted TCN of the packet. Topology Change Notification (TCN) is a BPDU that a bridge sends out to its root port to signal a topology change. If set to *True*, it stops the port from propagating received TCN and to other ports. The default value is *False*.

Click **Apply** for the settings to take effect. Click **Refresh** to renew the page.

## QoS > Storm Control

The Storm Control feature provides the ability to control the receive rate of broadcast, multicast, and unknown unicast packets. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided.

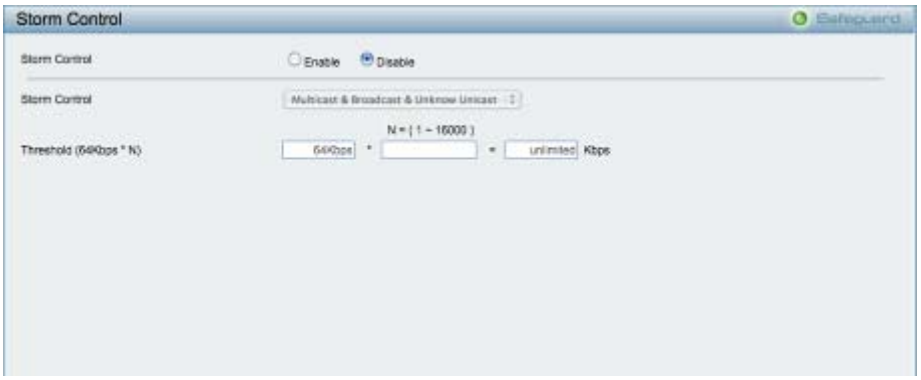


**Figure 71 – QoS > Storm Control**

**Storm Control Type:** User can select the different Storm type from Broadcast Only, Multicast & Broadcast, and Multicast & Broadcast & Unknown Unicast.

**Threshold (64Kbps * N):** If storm control is enabled (default is disabled), the threshold is from of 64 ~ 1,024,000 Kbit per second, with steps (N) of 64Kbps. N can be from 1 to 16000.

Click **Apply** for the settings to take effect.

## QoS > Bandwidth Control

The Bandwidth Control page allows network managers to define the bandwidth settings for a specified port's transmitting and receiving data rates.

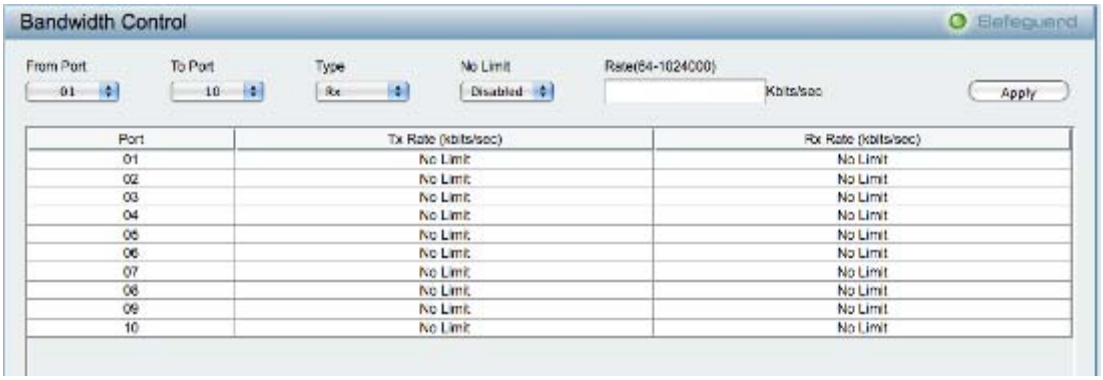


**Figure 72 – QoS > Bandwidth Control**

**From Port / To Port:** A consecutive group of ports may be configured starting with the selected port.
**Type:** This drop-down menu allows you to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
**No Limit:** This drop-down menu allows you to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.
**Rate (64-1024000):** This field allows you to enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 64 and 1024000.

Click **Apply** to set the bandwidth control for the selected ports.

## QoS > 802.1p/DSCP Priority Settings

QoS is an implementation of the IEEE 802.1p standard that allows network administrators to reserve bandwidth for important functions that require a larger bandwidth or that might have a higher priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Thus with larger bandwidth, less critical traffic is limited, and therefore excessive bandwidth can be saved.

The following figure displays the status of Quality of Service priority levels of each port, higher priority means the traffic from this port will be first handled by the switch. For packets that are untagged, the switch will assign the priority depending on your configuration.

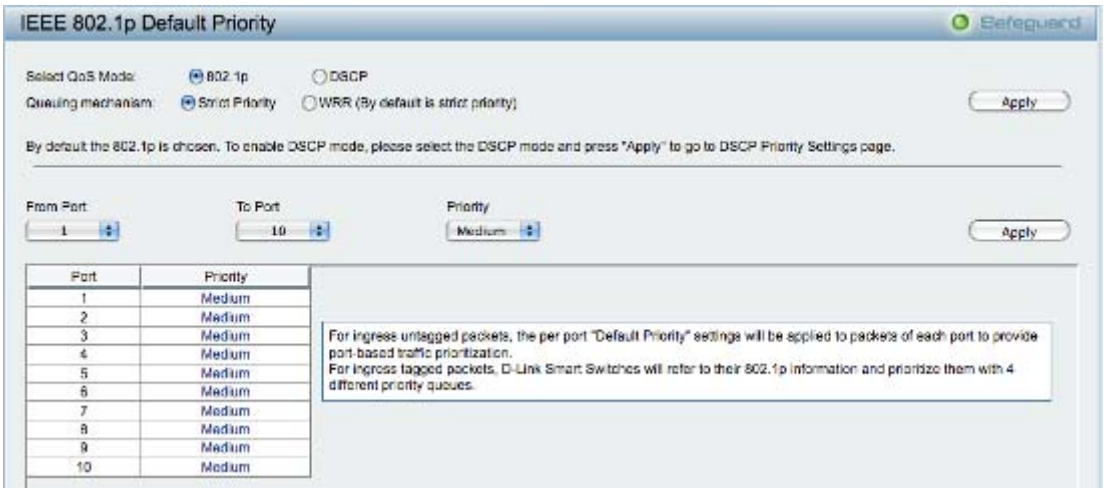


**Figure 73 – QoS > 802.1p Default Priority**

By selecting the DSCP priority, the web pages will changes as seen below:

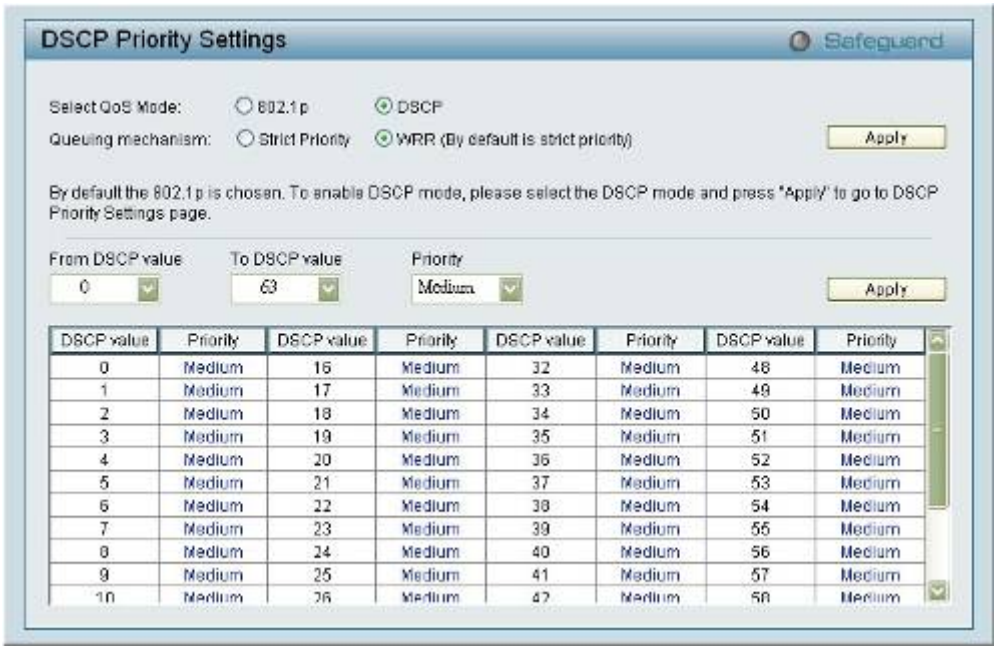
DSCP Priority Settings
Safeguard
Select QoS Mode: 802.1p DSCP
Queuing mechanism: Strict Priority WRR (By default is strict priority)
Apply
By default the 802.1p is chosen. To enable DSCP mode, please select the DSCP mode and press "Apply" to go to DSCP Priority Settings page.
From DSCP value
To DSCP value
Priority
0
63
Medium
Apply
DSCP value Priority DSCP value Priority DSCP value Priority DSCP value Priority
0 Medium 16 Medium 32 Medium 48 Medium
1 Medium 17 Medium 33 Medium 49 Medium
2 Medium 18 Medium 34 Medium 50 Medium
3 Medium 19 Medium 35 Medium 51 Medium
4 Medium 20 Medium 36 Medium 52 Medium
5 Medium 21 Medium 37 Medium 53 Medium
6 Medium 22 Medium 38 Medium 54 Medium
7 Medium 23 Medium 39 Medium 55 Medium
8 Medium 24 Medium 40 Medium 56 Medium
9 Medium 25 Medium 41 Medium 57 Medium

**Figure 74 – QoS > DSCP Priority Settings**

**Select QoS Mode:** D-Link Smart Switch allows the user to prioritize the traffic based on the 802.1p priority in the VLAN tag or the DSCP (Differentiated Services Code Point) priority in the IP header. Only one mechanism is selected to prioritize the packets at a time.

**Queuing Mechanism:** Select Strict Priority to process the packets with the highest priority first. Select WRR (Weighted Round-Robin) to process packets according to the weight of each priority. When a priority level has reached its egress weight, the system will process the packets in the next level even if there are remaining packets. D-Link Smart Switch system's weight of priority levels are: 8 (Highest), 4 (High), 2 (Medium) and 1 (Low) packet. By default, the queuing mechanism is **Strict Priority**.

**Default Priority:** Default is **Medium**. In 802.1p QoS mode, you can use **From Port** / **To Port** to specify the default priority of each port. In DSCP mode, you can configure the global default priority value by using **From DSCP value** / **To DSCP value**.

## Security > Trusted Host

Use Trusted Host function to manage the switch from a remote station. You can enter up to ten designated management stations networks by defining the IP address/Subnet Mask as seen in the figure below.

Trusted Host
Safeguard
Trusted Host: Enabled Disabled
Apply
Trusted Host Settings
( Maximum Entries : 10 )
ID IP Address IP Mask Delete
Input the permitted IP Address/Mask in below window, the format can be either 192.168.1.1/255.255.255.0 or 192.168.1.1/24
Add Host
IP Address / IP Mask
Cancel
Apply
Note: Create a list of IP Addresses that can access the switch. Your local host IP Addresses must be one of the IP Addresses to avoid disconnection.

**Figure 75 Security > Trusted Host**

To define a management station IP setting, click the **Add Host** button and type in the IP address and Subnet mask. Click the **Apply** button to save your settings. You may permit only single or a range of IP addresses by different IP mask settings, the format can either be 192.168.1.1/255.255.255.0 or 192.168.0.1/24. Please see the example below for permitting the IP range

| IP Address | Subnet Mask | Permitted IP |
|---|---|---|
| 192.168.0.1 | 255.255.255.0 | 192.168.0.1~192.168.0.255 |
| 172.17.5.215 | 255.0.0.0 | 172.0.0.1~172.255.255.255 |

To delete the IP address, simply click the **Delete** button. Check the unwanted address, and then click **Apply**.

**Security > Safeguard Engine**

D-Link's **Safeguard Engine** is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps protect the Web-Smart Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.

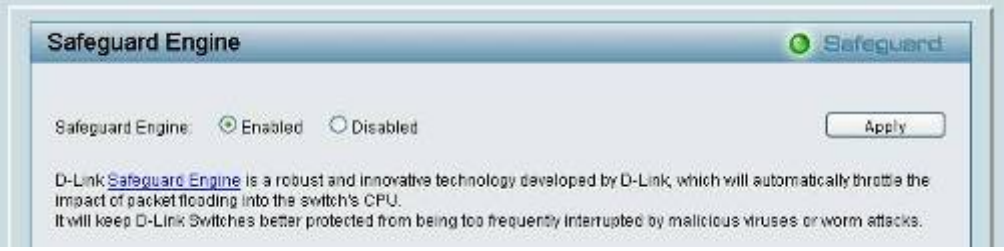
Safeguard Engine
Safeguard
Safeguard Engine:
Enabled
Disabled
Apply
D-Link Safeguard Engine is a robust and innovative technology developed by D-Link, which will automatically throttle the impact of packet flooding into the switch's CPU.
It will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.

**Figure 76 – Security > Safeguard Engine**

**Security > Port Security**

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to stopping auto-learning processing from gaining access to the network.

A given ports' (or a range of ports') dynamic MAC address learning can be stopped such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. Using the drop-down menu, change **Admin State** to *Enabled*, and then click **Apply** to confirm the setting.

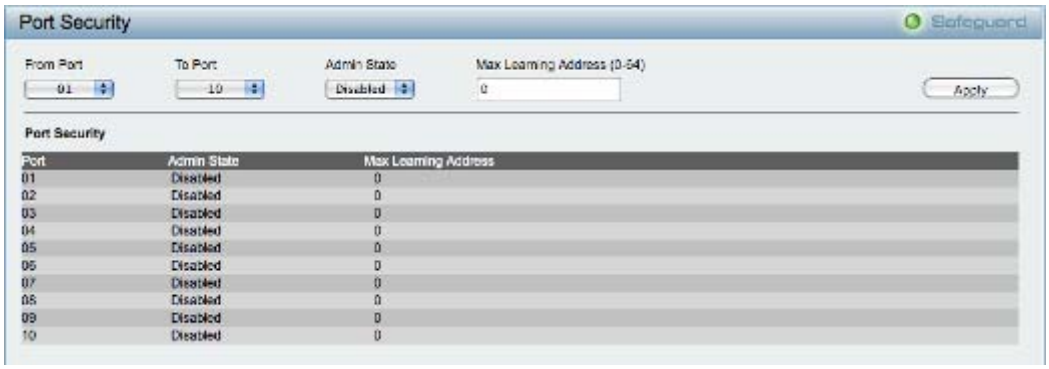


**Figure 77 – Security > Port Security**

**Security > 802.1X > 802.1X Settings**

Network switches provide easy and open access to resources, by simply attaching a client PC. Unfortunately this automatic configuration also allows unauthorized personnel to easily intrude and possibly gain access to sensitive data.

IEEE-802.1X provides a security standard for network access control, especially in Wi-Fi wireless networks. 802.1X holds a network port disconnected until authentication is completed. The switch uses Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol client identity (such as a user name) with the client, and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contains the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client

software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists.

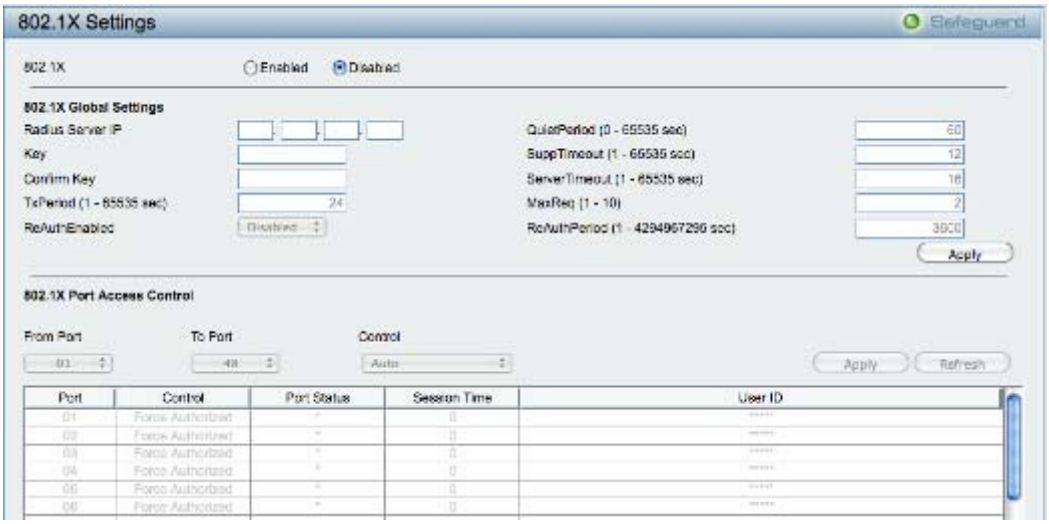


**Figure 78 – Security > 802.1X > 802.1X Setting**

By default, 802.1X is disabled. To use EAP for security, select enabled and set the 802.1X **Global Settings** for the Radius Server and applicable authentication information.

**RADIUS Server IP:** The IP address of the external Radius Server. You need to specify an RADIUS server to enable 802.1X authentication.

**Key:** Masked password matching the Radius Server Key. The max. length is 32 characters.

**Confirm Key:** Enter the Key a second time for confirmation.

**TxPeriod (1 – 65535 sec):** This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. Default is 24 seconds.

**ReAuthEnabled:** This function is to determine whether regular re-authentication will take place on this port(s). When the 802.1X function is enabled, the switch sends an EAP-request/identity packet to client. The ReAuthEnabled function is by default disabled.

**QuietPeriod (0 – 65535 sec):** Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default is 80 seconds

**SuppTimeout (1 – 65535 sec):** This value determines timeout conditions in the exchanges between the Authenticator and the client. Default is 12 seconds.

**ServerTimeout (1 – 65535 sec):** Sets the amount of time the switch waits for a response from the client before resending the response to the authentication server. Default is 16 seconds.

**MaxReq (1 – 10):** This parameter specifies the maximum number of times that the switch retransmits an EAP request (md-5challnege) to the client before it times out the authentication session. Default is 5 times.

**ReAuthPeriod (1 – 4294967295 sec):** This command affects the behavior of the switch only if periodic re-authentication is enabled. Default is 3600.

To establish 802.1X port-specific assignments, select the **From Ports** / **To Ports** and select **Enable**.

**802.1X Port Access Control:** Three type of Port Access Control State can be "**Force Authorized**", "**Force UnAuthorized**", and "**Auto**".

Select **Force Authorized** to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.

If **Force Unauthorized** is selected, the port will remain in the unauthorized state ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.

If **Auto** is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

The default setting is **Auto**.

**Security > MAC Address Table > Static MAC**

This feature provides two distinct functions. The **Disable Auto Learning** table allows turning off the function of learning MAC address automatically, if a port isn't specified as an uplink port (for example, connects to a DHCP Server or Gateway). By default, this feature is Off (disabled).

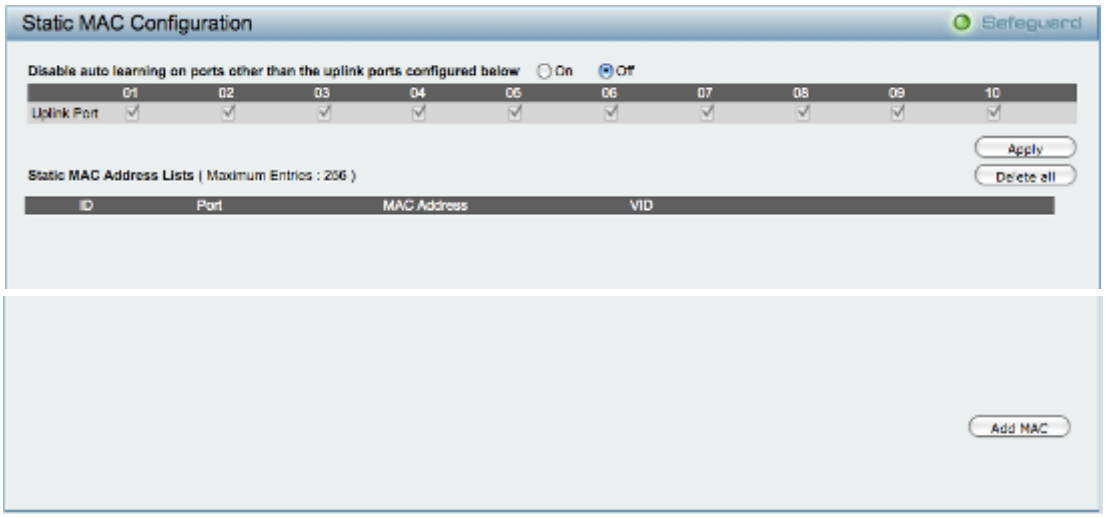


**Figure 79 – Security > Static Mac Address**

To initiate the removal of auto-learning for any of the uplink ports, click **On** to enable this feature, and then select the port(s) for auto learning to be disabled.

The **Static MAC Address Setting** table displays the static MAC addresses connected, as well as the VID. Click **Add Mac** to add a new MAC address, you also need to select the assigned Port number. Enter both the Mac Address and VID, and then Click **Apply**. Click **Delete** to remove one entry or click **Delete all** to clear the list. You can also copy a learned MAC address from the **Dynamic Forwarding Table** (please refer to **Security > MAC Address Table > Dynamic Forwarding Table** for details).

By disabling Auto Learning capability and specifying the static MAC addresses, the network is protected from potential threats like hackers, because traffic from illegal MAC addresses will not be forwarded by the Switch.

**Security > MAC Address Table > Dynamic Forwarding Table**

For each port, this table displays the MAC address learned by the Switch. To add a MAC address to the Static Mac Address List, click the **Add** checkbox, and then click **Apply** associated with the identified address.

**Figure 80 – Security > Dynamic Forwarding Table**

**Monitoring > Statistics**

The Statistics screen displays the status of each port packet count.

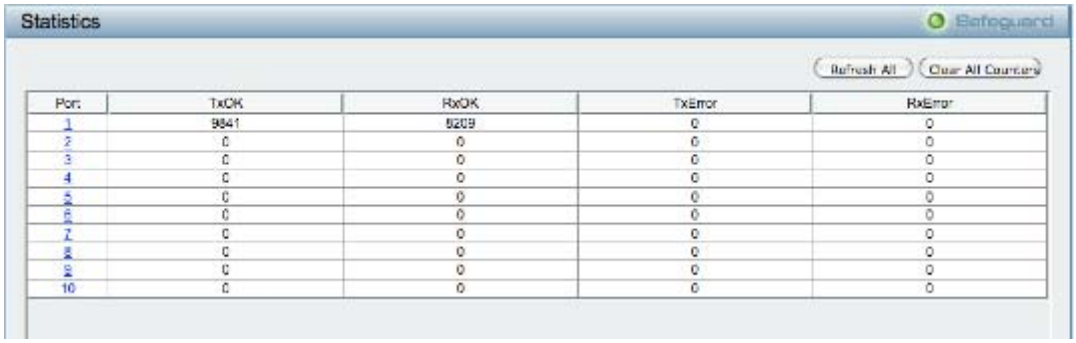


**Figure 81 – Monitoring > Statistics**

**Refresh All:** Renews the details collected and displayed.
**Clear All Counters:** To reset the details displayed.
**TxOK:** Number of packets transmitted successfully.
**RxOK:** Number of packets received successfully.
**TxError:** Number of transmitted packets resulting in error.
**RxError:** Number of received packets resulting in error.

To view the statistics of individual ports, click one of the linked port numbers for details.

**Figure 82 – Monitoring > Port Statistics**

**Previous Page:** Go back to the Statistics main page.
**Refresh:** To renew the details collected and displayed.
**Clear Counter:** To reset the details displayed.

**Monitoring > Cable Diagnostics**

The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.

Select a port and then click the **Test Now** button to start the diagnosis.

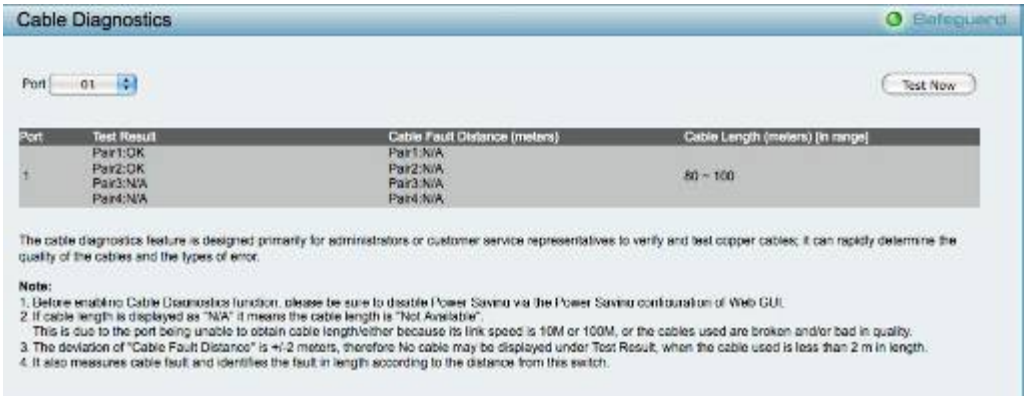
Cable Diagnostics
Safeguard
Port 01
Test Now
Port
Test Result
Cable Fault Distance (meters)
Cable Length (meters) [in range]
1
Pair1:OK
Pair2:OK
Pair3:N/A
Pair4:N/A
Pair1:N/A
Pair2:N/A
Pair3:N/A
Pair4:N/A
80 ~ 100
The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.
Note:
1. Before enabling Cable Diagnostics function, please be sure to disable Power Saving via the Power Saving configuration of Web GUI.
2. If cable length is displayed as "N/A" it means the cable length is "Not Available".
This is due to the port being unable to obtain cable length/either because its link speed is 10M or 100M, or the cables used are broken and/or bad in quality.
3. The deviation of "Cable Fault Distance" is +/-2 meters, therefore No cable may be displayed under Test Result, when the cable used is less than 2 m in length.
4. It also measures cable fault and identifies the fault in length according to the distance from this switch.

**Figure 83 – Monitoring > Cable Diagnostic**

**Test Result:** The description of the cable diagnostic results.

- **OK** means the cable is good for the connection.
- **Short in Cable** means the wires of the RJ45 cable may be in contact somewhere.
- **Open in Cable** means the wires of RJ45 cable may be broken, or the other end of the cable is simply disconnected.
- **Test Failed** means some other errors occurred during cable diagnostics. Please select the same port and test again.

**Cable Fault Distance (meters):** Indicates the distance of the cable fault from the Switch port, if the cable is less than 2 meters, it will show “No Cable”.

**Cable Length (meter):** If the test result shows OK, then cable length will be indicated for the total length of the cable. The cable lengths are categorized into four types: <50 meters, 50~80 meters, 80~100 meters and >100 meters.

**NOTE:** Cable length detection is effective on Gigabit ports only.

**NOTE:** Please be sure that Power Saving feature is disabled before enabling Cable Diagnostics function.

**Monitoring > System Log**

The System Log page provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.

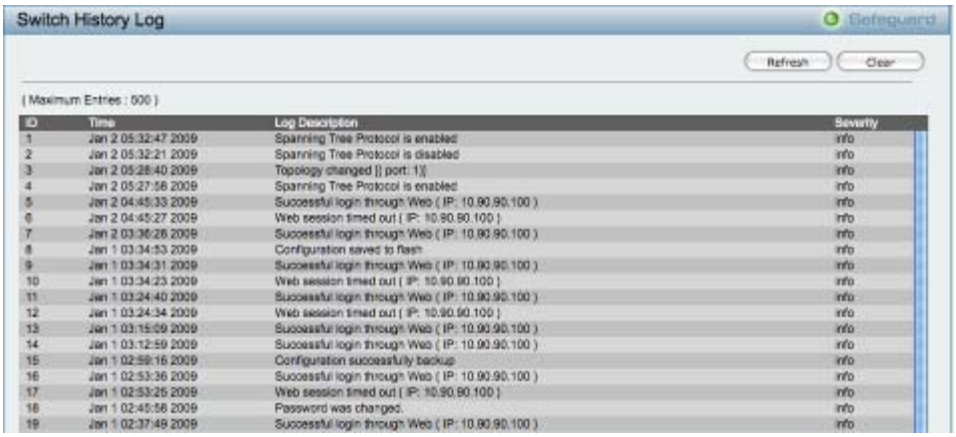
Switch History Log
Safeguard
Refresh
Clear
( Maximum Entries : 500 )
ID Time Log Description Severity
1 Jan 2 05:32:47 2009 Spanning Tree Protocol is enabled info
2 Jan 2 05:32:21 2009 Spanning Tree Protocol is disabled info
3 Jan 2 05:28:40 2009 Topology changed [] port: 1)[ info
4 Jan 2 05:27:56 2009 Spanning Tree Protocol is enabled info
5 Jan 2 04:45:33 2009 Successful login through Web ( IP: 10.90.90.100 ) info
6 Jan 2 04:45:27 2009 Web session timed out ( IP: 10.90.90.100 ) info
7 Jan 2 03:36:26 2009 Successful login through Web ( IP: 10.90.90.100 ) info
8 Jan 1 03:34:53 2009 Configuration saved to flash info
9 Jan 1 03:34:31 2009 Successful login through Web ( IP: 10.90.90.100 ) info
10 Jan 1 03:34:23 2009 Web session timed out ( IP: 10.90.90.100 ) info
11 Jan 1 03:24:40 2009 Successful login through Web ( IP: 10.90.90.100 ) info
12 Jan 1 03:24:34 2009 Web session timed out ( IP: 10.90.90.100 ) info
13 Jan 1 03:15:09 2009 Successful login through Web ( IP: 10.90.90.100 ) info
14 Jan 1 03:12:59 2009 Successful login through Web ( IP: 10.90.90.100 ) info
15 Jan 1 02:59:16 2009 Configuration successfully backup info
16 Jan 1 02:53:36 2009 Successful login through Web ( IP: 10.90.90.100 ) info
17 Jan 1 02:53:25 2009 Web session timed out ( IP: 10.90.90.100 ) info
18 Jan 1 02:45:58 2009 Password was changed. info
19 Jan 1 02:37:49 2009 Successful login through Web ( IP: 10.90.90.100 ) info

**Figure 84 – Monitoring > System Log**

**ID:** Displays an incremented counter of the System Log entry. The Maximum entries are 500.

**Time:** Displays the time in days, hours, and minutes the log was entered.

**Log Description:** Displays a description event recorded.

**Severity:** Displays a severity level of the event recorded.

Click **Refresh** to renew the page, and click **Clear** to clean out all log entries.

## ACL > ACL Configuration Wizard

Access Control List (ACL) allows you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. This criterion can be specified on a basis of the MAC address, or IP address.

The ACL Configuration Wizard will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically. The maximum usable profiles are 50 and with 240 Rules in total for the switch.

**Figure 85 – ACL > ACL Configuration Wizard**

**From:** Specify the origin of accessible packets. The possible values are:

**Any -** Indicates ACL action will be on packets from any source.

**MAC Address -** Indicates ACL action will be on packets from this MAC address.

**IPv4 Addresses -** Indicates ACL action will be on packets from this IPv4 source address.

**To:** Specify the destination of accessible packets. The possible values are:

**Any -** Indicates ACL action will be on packets from any source.

**MAC Address -** Indicates ACL action will be on packets from this MAC address. The field of format is xx-xx-xx-xx-xx-xx.

**IPv4 Addresses -** Indicates ACL action will be on packets from this IPv4 source address.

**Service Type:** Specify the type of service. The possible values are:

**Any** - Indicates ACL action will be on packets from any service type.

**Ether type** - Specifies an Ethernet type for filtering packets.

**ICMP All** - Indicates ACL action will be on packets from ICMP packets.

**IGMP** - IGMP packets can be filtered by IGMP message type.

**TCP All** - Indicates ACL action will be on packets from TCP Packets.

**TCP Source Port** - Matches the packet to the TCP Source Port.

**TCP Destination Port** - Matches the packet to the TCP Destination Port.

**UDP All** - Indicates ACL action will be on packets from UDP Packets.

**UDP Source Port** - Matches the packet to the UDP Source Port.

**UDP Destination Port** - Matches the packet to the UDP Destination Port.

**Action:** Specify the ACL forwarding action matching the rule criteria. *Permit* forwards packets if all other ACL criteria are met. *Deny* drops packets if all other ACL criteria is met.

**Port:** Enter a range of ports to be configured.

Press **Apply** for the settings to take effect.

**NOTE:** Once the ACL rules conflict, rules with the smaller rule ID will take higher priority.

**NOTE:** Be careful when configuring ACL rules, an inappropriate ACL rule may cause management access failure.

**ACL > ACL Profile List**

The ACL Profile List provides information for configuring ACL Profiles manually. ACL profiles are attached to interfaces, and define how packets are forwarded if they match the ACL criteria.

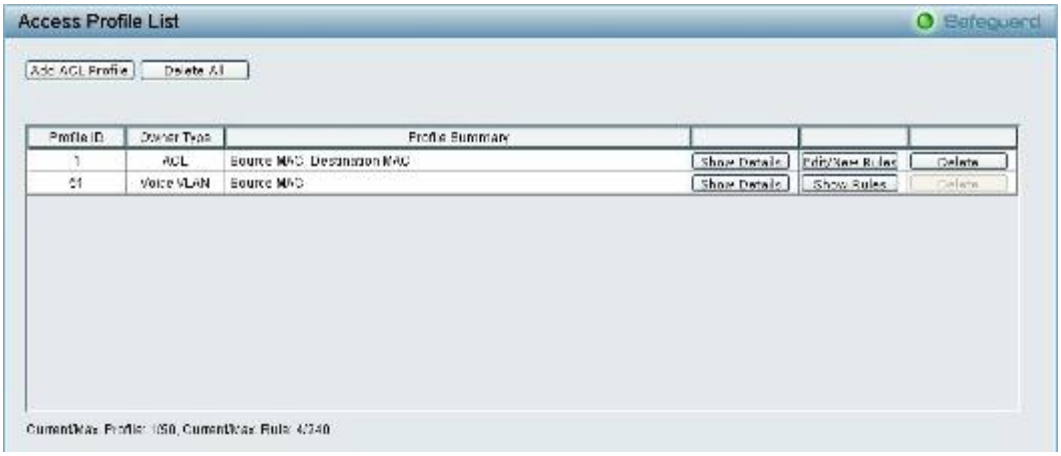


**Figure 86 – ACL > ACL Profile List**

The contents of Access Profile List table include:

**Profile ID:** Indicates the profile Identification number. The possible configured profile IDs are 1~50, and profile ID 51 is reserved for Voice VLAN.

**Owner Type:** The owner type of ACL profile; it can be normal ACL or Voice VLAN.

**Profile Summary:** Displays the profile summary.

**Show Details:** To display an ACL's profile details. The ACL profile details are displayed below the ACL table.

**Show Rules:** To show the access rule in this profile.

**Edit / New Rules:** To edit or create an access rule in this profile. To add a new rule, please see **Access Rule List** in the next section.

**Delete:** To delete an access profile.

To manually add a profile, click **Add ACL Profile**:

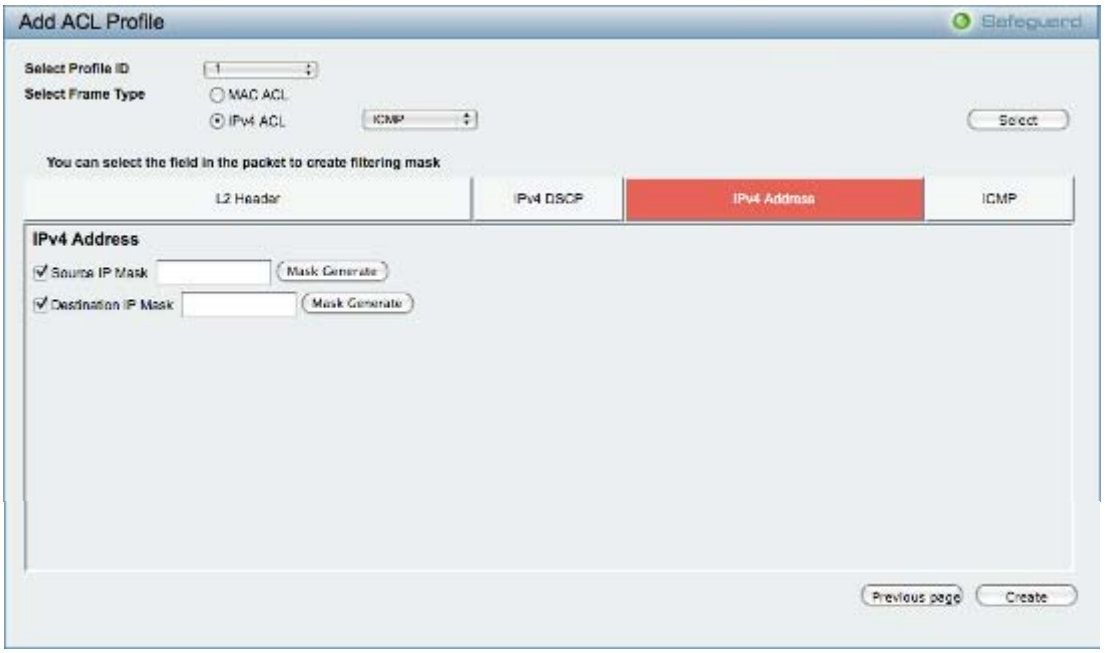


**Figure 87 – Add Access Profile**

The steps of adding an access profile are described below:

1) After selecting the **Profile ID** and **Frame Type** (MAC or IPv4), specify attributes like Untagged/Tagged (for MAC), or ICMP/IGMP/TCP/UDP (for IPv4). Click *Select* and a simplified frame diagram will be displayed.

2) Selecting the field of interest will display the related columns in the lower part of the page. Enter the filtering mask and click **Create** when done. A filtering mask is to specify the digit that you want to check. For example, if you want to check a network of 192.168.1.0/24, then you should enter the IP mask as 255.255.255.0.

**NOTE:** You cannot select Payload in a MAC ACL, or L2 Header in IP ACL.

3) After the **Profile ID** has been created, it will go back to the main Access Profile List page, clicking the **Edit / New Rules** button to enter the **Access Rule List** page.

**Figure 88 – Access Rule List**

**Profile ID:** Indicates the corresponding access profile Identification number.
**Access ID:** Indicates the access rule Identification number.
**Profile Type:** Displays the profile type.
**Summary:** Displays the access rule summary.
**Action:** Displays the access rule action.

To add a new rule, click **Add Rule**:

**Figure 89 – Add Access Rule**

**Profile Information** displays the information to which the rule is being added to, including **Profile ID** and other fields specified.

In **Rule Detail**, you can specify the details of an access rule. Below are all the possible parameters that can be set.

**Access ID:** Specify the Access ID (1-65535).
**Type:** Display the type of rule.
**VLAN ID:** The VLAN ID for a previously configured VLAN.
**Destination MAC Address:** Specify the Destination MAC address, the field of format is xx-xx-xx-xx-xx-xx.
**Source MAC Address:** Specify the Source MAC address, the field of format is xx-xx-xx-xx-xx-xx.
**802.1p:** Specify the 802.1p priority value.
**Ether Type:** Specify the Ethernet Type value.
**Destination IP Address:** Specify the Destination IP address.
**Source IP Address:** Specify the Source IP address.
**DSCP:** Specify the DSCP value.
**IP Protocol:** The L4 protocol above IP. Possible values are ICMP, IGMP, TCP, and UDP.
**ICMP Type:** Specify the ICMP packet type.
**ICMP Code:** Specify the ICMP packet Code.
**IGMP Type:** Specify the IGMP packet type.
**Source Port:** Specify the TCP or UDP source port value.
**Destination Port:** Specify the TCP or UDP destination port value.
**TCP Flag:** Specify the TCP flag value.
**Ports:** Specify the switch ports that you want to implement the access rule to.
**Action:** Specify the ACL forwarding action matching the rule criteria. **Permit** forwards packets if all other ACL criteria are met. **Deny** drops packets if all other ACL criteria is met.

Click **Apply** to make it effective.

**NOTE:** The switch begins the access rule with the smallest access ID, so be careful in assigning the ID for the expected results.

To modify an existing rule, please click on the Access ID hyperlink.

**Figure 90 – ACL > Access Profile List > Access Rule List**

## ACL > ACL Finder

This page is used to help find a previously configured ACL entry. To search for an entry, enter the profile ID from the drop-down menu, select a port that you wish to view, define the state and click **Find.** The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.

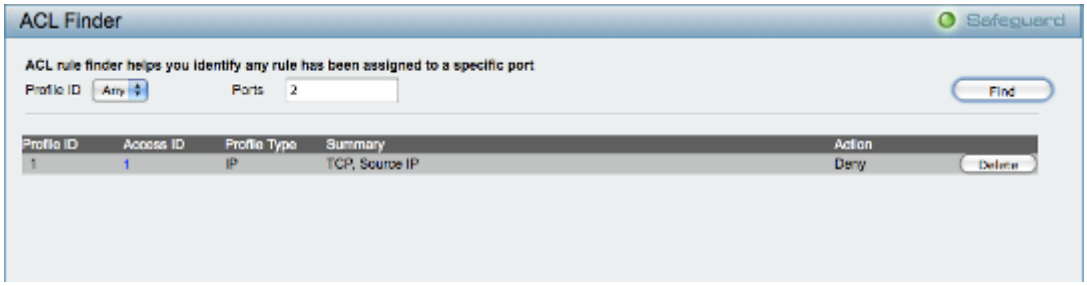


**Figure 91 – ACL > ACL Finder**

## PoE > PoE Port Settings

DGS-1210-10P supports Power over Ethernet (PoE) as defined by the IEEE 802.3at specification. Ports 1-8 can supply 54VDC power to PDs (Powered Device) over Category 5 or Category 3 UTP Ethernet cables. DGS-1210-10P follows the standard PSE (Power Supply Equipment) pinout Alternative A, whereby power is sent out over pins 1, 2, 3 and 6.

DGS-1210-10P works with all D-Link 802.3af or 802.3at capable devices. The Switch also works in PoE mode with all non-802.3af capable D-Link AP, IP Cam and IP phone equipment via the PoE splitter DWL-P50.

IEEE 802.3at defined that the PSE provides power according to the following classification:

| Class | Usage | Output power limit by PSE |
|---|---|---|
| 0 | Default | 15.4W |
| 1 | Optional | 4.0W |
| 2 | Optional | 7.0W |
| 3 | Optional | 15.4W |
| 4 | Reserved | 30W |

The PoE port table will display the PoE status including, Port Enable, Power Limit, Power (W), Voltage (V), Current (mA), Classification, Port Status. You can select **From Port** / **To Port** to control the PoE functions of a port. DGS-1210-10P will auto disable the ports if port current is over 375mA in 802.3af mode or 625mA in pre-802.3at mode while other ports remain active

**Note:** The PoE Status information of Power current, Power Voltage, and Current is the power usage information of the connected PD; please "Refresh" to renew the information.

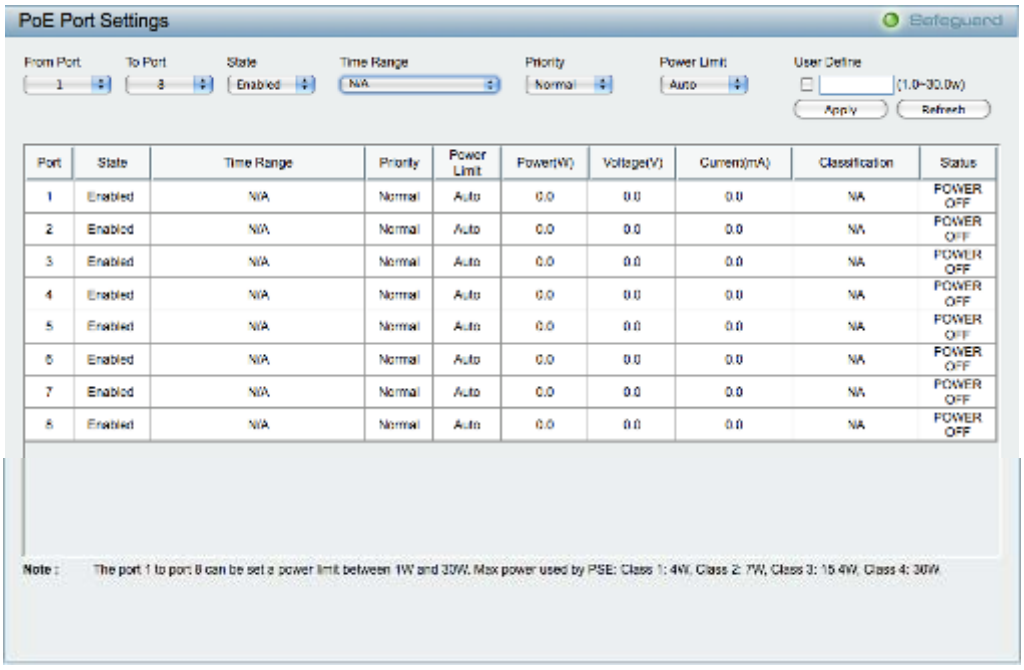


**Figure 92 – PoE > PoE Port Setting**

**State:** Select “Enabled” or “Disabled” to configure PoE function for designated port(s). Default is **Enabled**.

**Time Range:** Select the PoE time profile configured from Time-Based PoE > Time Range Settings to enable the time-based PoE function on designated port(s). Default setting is **N/A**.

**Priority:** Configure the power supply priority as “Low”, “Normal”, or “High” on designated port(s). Default is **Normal**.

**Power Limit:** This function allows you to manually set the port power current limitation to be given to the PD. To protect the DGS-1210-10P and the connected devices, the power limit function will disable the PoE function of the port when the power is overloaded. Select from "**Class 1**", "**Class 2**", "**Class 3**", **“Class 4”** and "**Auto**" for the power limit. "**Auto**" will negotiate and follow the classification from the PD power current based on the 802.3at standard.

**User Define:** Check the box and input the power budget (from 1 to 30W) to manually assign an upper limit of port power budget on designated port(s).

## PoE > PoE System Settings

This page will display the PoE status including System Budget Power, Support Total Power, Remainder Power, and The ratio of system power supply.

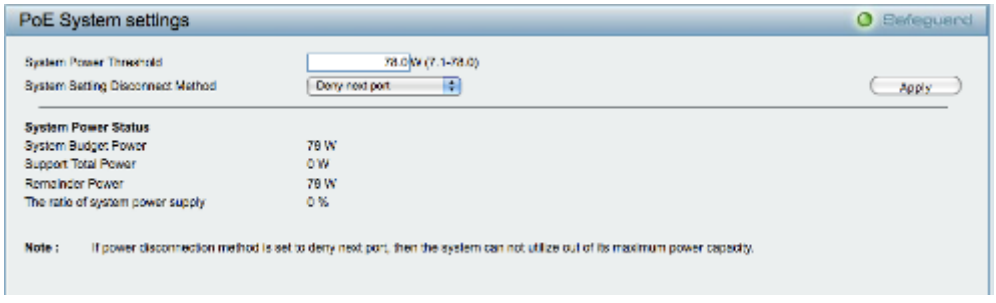


**Figure 93 – PoE > PoE System Setting**

**System Power Threshold:** Manually configure the system power budget (7.1 ~ 78.0 W)

**System Setting Disconnection Method:** Configure PoE power management mode. The power management policy will deny powering to low priority port while system power budget is not enough to supply power. DGS-1210-10P support two deny policies, *Deny next port and Deny low priority*. The Deny next port means the port with earliest plug-in PD gets the highest priority, whereas the latest gets the lowest priority.

And the Deny low priority port applied the port priority setting configured from PoE port setting page. Default setting is **Deny next port**.

**Note:** The power management policy is only effective while PoE system entering guard band mode (0 < remainder power <= 7).

## Time-Based PoE > Time Range Settings

The Time Range window is used in conjunction with the PoE feature to determine the powering time range based on days of the week when PoE is enabled on the Switch port. Once it is configured here, the time range settings will be applied to the PoE port setting.

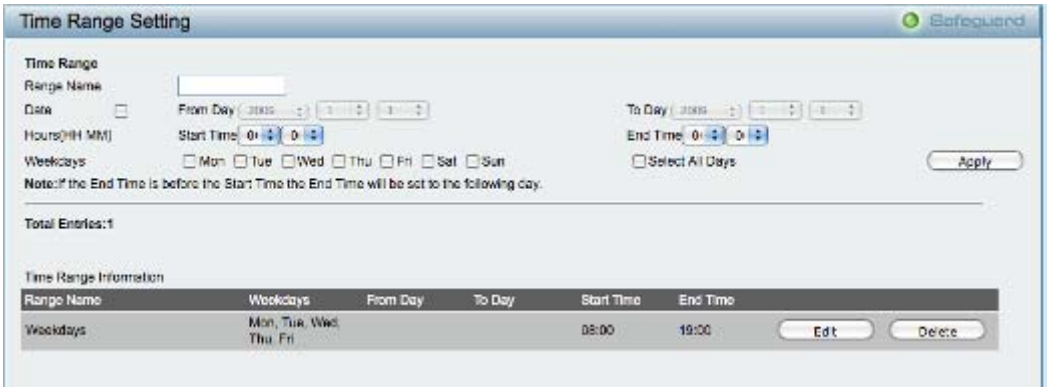


**Figure 94 – Time-Based PoE > Time Range Settings**

**Range Name:** Name of a time range profile.

**Date:** Select the checkbox if there is a certain date range for the profile to use. Select from drop-down menu of **From Day** and **To Day** to define the date range.

**Hours:** Select from drop-down menu of **Start Time** and **End Time** to define the range of a day. Note: If the End Time is before the Start Time the End date should be set to the following day.

**Weekdays:** Select the checkboxes for the days you want to apply the time range profile per week. You can select all days.

Click **Apply** to confirm profile creation.

## LLDP > LLDP Global Settings

**LLDP (Link Layer Discovery Protocol)** provides IEEE 802.1AB standards-based method for switches to advertise themselves to neighbor devices, as well as to learn about neighbor LLDP devices. DGS-1210-10P will keep the information in the Management Information Base (MIB). SNMP utilities can learn the network topology by obtaining the MIB information in each LLDP device. The LLDP function is enabled by default.

The DGS-1210-10P and DWL-3140AP can be centrally managed and discovered via the optional D-Link Smart WLAN Manager.

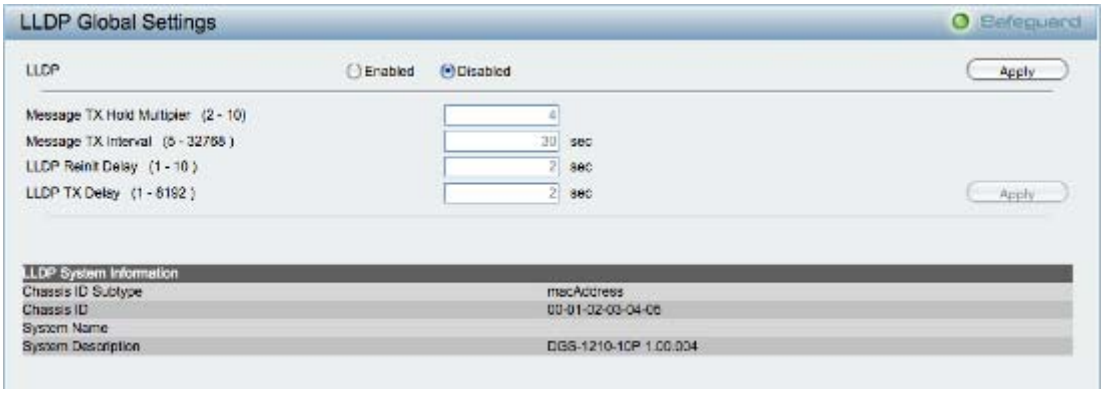


**Figure 95 –LLDP > LLDP Global Settings**

**LLDP:** When this function is *Enabled*, the switch can start to transmit, receive and process the LLDP packets. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. Click **Apply** to make the change effective.

**Message TX Hold Multiplier (2-10):** This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is **4**.

**Message TX Interval (5-32768):** This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is **30** seconds.

**LLDP ReInit Delay (1-10):** This parameter indicates the amount of delay from the time adminStatus becomes "disabled" until re-initialization is attempted. The default value is **2** seconds.

**LLDP TX Delay (1-8192):** This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula: 1 < txDelay < (0.25 °— msgTxInterval). The default value is **2** seconds.

## LLDP > LLDP Remote Port Information

This page is used to display the LLDP Remote Port Brief Table. Click **Show Normal** to display additional information.

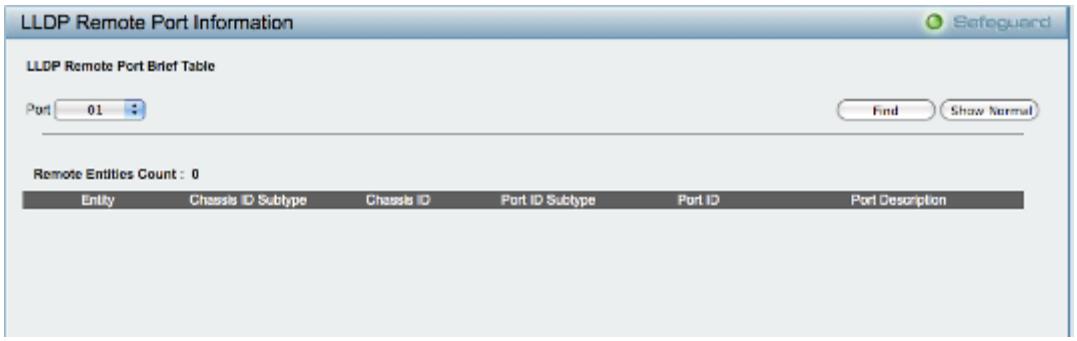


**Figure 96 –LLDP > LLDP Remote Port Information**

## LLDP > LLDP MED Settings

By selecting a range of ports (**From Port** and **To Port**), the power PSE TLV type can be enabled for all selected ports to indicate the power source equipment (PSE) switch to transmit high power (15.4 to 30 Watts) to the pre-standard of 802.3at power devices via LLDP MDI TLV. Through this feature, the PSE can provide precise output power to the pre-standard of 802.3at power devices and achieve optimal power management.

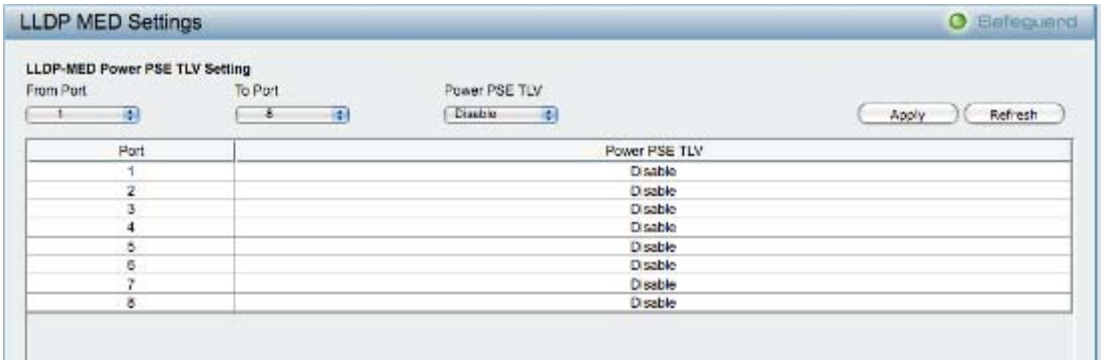


**Figure 97 –LLDP > LLDP MED Settings**

# 6 Command Line Interface

The D-Link Web Smart Switch allows a computer or terminal to perform some basic monitoring and configuration tasks by using the Command Line Interface (CLI) via TELNET protocol.

## To connect a switch via TELNET:

1. Make sure the network connection between the switch and PC is active.
2. To connect, launch any terminal software like ***HyperTerminal*** in Microsoft Windows, or just use the command prompt by typing the command *telnet* followed by the switch IP address, eg. *telnet 10.90.90.90*.
3. The logon prompt will appear.

## Logging on to the Command Line Interface:

Enter your User Name and Password to log in. The default user name and password is **admin**. Note that the user name and password are case-sensitive. Press **Enter** in both the Username and Password fields. The command prompt will appear as shown below (**DGS-1210-10P>):**

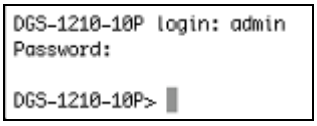


**Figure 98 – Command Prompt**

The user session is automatically terminated if idle for the login timeout period. The default login timeout period is 5 minutes. To change the login timeout session, please refer to chapter 5.

## CLI Commands:

There are a number of helpful features included in the CLI. Entering the **?** command will display a list of commands.

**Figure 99 – The ? Command**

### Download

The **download** command is used to download and install new firmware or a Switch configuration file from a TFTP server.

**Syntax**

**download** { firmware_fromTFTP tftp://ip-address/filename | cfg_fromTFTP tftp://ip-address/filename}

**Parameters**

| Parameter | Description |
|---|---|

| | |
|---|---|
| firmware_fromTFTP | Download and install new firmware on the Switch from a TFTP server. |
| cfg_fromTFTP | Download a switch configuration file from a TFTP server. |
| tftp://ip-address/ | The IP address of the TFTP server. |
| filename | The filename of the firmware or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not at the root directory of the TFTP server. |

**Upload**

The **upload** command is used to upload the firmware file or a Switch configuration file to a TFTP server.

**Syntax**

**upload** { firmware_toTFTP tftp://ip-address/filename | cfg_toTFTP tftp://ip-address/filename }

**Parameters**

| Parameter | Description |
|---|---|
| firmware_toTFTP | Upload the firmware on the Switch from a TFTP server. |
| cfg_toTFTP | Specifies that the Switch's current settings will be uploaded to the TFTP server. |
| tftp://ip-address/ | The IP address of the TFTP server. |
| filename | The filename of the firmware or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not at the root directory of the TFTP server. |

**Config ipif System**

The **config ipif System** command sets the IP address of the switch.

**Syntax**

**config ipif System** { ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp }

**Parameter**

| Parameter | Description |
|---|---|
| ipaddress <ip-address> <subnet-mask> | The IP address and subnet mask to be created. Users need to specify the address and mask information using the traditional format (for example,10.1.2.3/255.0.0.0). |
| gateway <gw-address> | The IP address of the router or gateway. |
| dhcp | Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface. |

**Logout**

This command closes the current connection.

**Syntax**

**logout**

**NOTE:** Save your configuration changes before logging out.

**Ping**

This command checks if another computer is on the network and listens for connections. You can ping the switch from any IP workstation the switch is connected to through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the switch and the workstation. The terminal interface sends five pings to the target station.

**Syntax**

**ping** <ipaddr>

**Parameter**

| Parameter | Description |
|---|---|
| <ipaddr> | The IP address of the target station. |

**Reboot**

This command reboots the system. All network connections are terminated and the boot code executes.

**Syntax**

**reboot**

**Reset**

All configurations will be reset to the default settings.

**Syntax**

**reset** config

**Show ipif**

The command displays the current IP address of the switch.

**Syntax**

**show ipif**

**Example**

```
DGS-1210-10P> show ipif
IP Setting Mode                 : Static
IP Address                      : 10.90.90.90
Subnet Mask                     : 255.0.0.0
Default Gateway                 : 0.0.0.0
```

**Figure 100 – The show ipif Command**

**Show switch**

The command displays the status of the switch.

**Syntax**

**show switch**

**Example**

```
DGS-1210-10P> show switch
System name                      :
System Contact                   :
System Location                  :
System up time                   : 0 days, 1 hrs, 43 min, 40 secs
System Time                      : 01/01/2009 02:43:38
System hardware version          : A1
System firmware version          : 1.00.004
System boot version              : 1.00.001
System Protocol version          : 2.001.004
System serial number             : 1MB1733K0000A
MAC Address                      : 00-01-02-03-04-05
```

**Figure 101 – The show switch Command**

## Config account admin password

The command sets the administrator password.

**Syntax**

**`config account admin password`** `<passwd>`

**Parameter**

| Parameter | Description |
|---|---|
| `<passwd>` | The new password of the administrator. |

## Save

The command saves the configuration changes to the memory.

**Syntax**

**`save`**

**Example**

```
DGS-1210-10P> save
Building configuration ...
[OK]
```

**Figure 102 – The save Command**

# *Appendix A - Ethernet Technology*

This chapter will describe the features of the D-Link Web Smart Switch and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

## *Gigabit Ethernet Technology*

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, and management objects, but with a tenfold increase in theoretical throughput of over 100-Mbps Fast Ethernet and a hundredfold increase over 10-Mbps Ethernet. Since it is compatible with all 10-Mbps and 100-Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting existing investments in hardware, software, or trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential in solving network bottlenecks, which frequently develops as more advanced computer users and newer applications continue to demand greater network resources. Upgrading key components, such as backbone connections and servers to Gigabit Ethernet technology, can greatly improve network response times as well as significantly speed up the traffic between subnets.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. With expected advances in the coming years in silicon technology and digital signal processing, which will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, a flexible foundation for the next generation of network technology products will be created. This will outfit your network with a powerful 1000-Mbps-capable backbone/server connection.

## *Fast Ethernet Technology*

The growing importance of LANs, and the increasing complexity of desktop computing applications, are fueling the need for high performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The non-disruptive and smooth evolution nature, and the dominating potential market base, virtually guarantees cost-effective and high performance Fast Ethernet solutions.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the CSMA/CD Ethernet protocol. Since the 100Mbps Fast Ethernet is compatible with all other 10Mbps Ethernet environments, it provides a straightforward upgrade and utilizes existing investments in hardware, software, and personnel training.

## *Switching Technology*

Another approach to push beyond the limits of Ethernet technology is the development of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments, which won't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this the total network capacity is multiplied, while still maintaining the same network cabling and adapter cards.

# *Appendix B - Technical Specifications*

## *Hardware Specifications*

### Key Components / Performance

- Switching Capacity:
  - DGS-1210-10P: 20Gbps
- Max. Forwarding Rate
  - DGS-1210-10P: 14.88Mpps
- Forwarding Mode: Store and Forward
- Packet Buffer memory:
  - DGS-1210-10P: 512K Bytes
- DDRII for CPU: 64M Bytes
- Flash Memory: 16M Bytes

### Port Functions

- 10 1000Base-T ports compliant with the following standards:
  - IEEE 802.3
  - IEEE 802.3u
  - Supports Full-Duplex operations
- 2 combo SFP ports compliant with the following standards:
  - IEEE 802.3z
  - Supports Full-Duplex operations
- SFP transceivers supported
  - DEM-310GT (1000BASE-LX, 10km)
  - DEM-311GT (1000BASE-SX, 550m)
  - DEM-314GT (1000BASE-LH, 50km)
  - DEM-315GT (1000BASE-ZX, 80km)
  - DEM-312GT2 (1000BASE-SX, 2km)
  - DEM-210 (100BASE-FX, 15km)
  - DEM-211 (100BASE-FX, 2km)

  WDM Transceivers Supported:
  - DEM-330T (1000Base-BX,TX-1550/RX-1310nm, 10km)
  - DEM-330R (1000Base-BX,TX-1310/RX-1550nm, 10km)
  - DEM-331T (1000Base-BX,TX-1550/RX-1310nm, 40km)
  - DEM-331R (1000Base-BX,TX-1310/RX-1550nm, 40km)
  - DEM-220T (100Base-BX, TX-1550/RX-1310nm, 20km)
  - DEM-220R (100Base-BX, TX-1310/RX-1550nm, 20km)

### Physical & Environment

- AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- Acoustic Value:
  - DGS-1210-10P: 0dB (Fan-less)
- Operation Temperature 0~40°C
- Storage Temperature -10~70°C
- Operation Humidity: 10%~95% RH
- Storage Humidity: 5%~95% RH

### Emission (EMI) Certifications

- FCC class A
- CE Class A
- VCCI Class A

### Safety Certifications

- cUL, LVD

## *Features*

### L2 Features

- Supports up to 8K MAC address
- Jumbo frame: Supports up to 10,000 bytes
- IGMP snooping: Supports 256 multicast group
- 802.1D Spanning Tree
- 802.1w Rapid Spanning Tree
- Loopback Detection
- 802.3ad Link Aggregation: up to 8 groups per device, up to 8 ports per group
- Port mirroring

### PoE Features

- PoE standard: Supports 802.3af and pre-standard of 802.3at
- PoE Capable Ports: All ports are selective at 15.4W or 30W per port, total 4 ports at 15.4W per port or 8 ports at 7.8W per port
- Power feeding for PoE: Port 1~8: Per port →Max is 30W, and the default is 15.4W
- PoE power budget: Output capacity for DGS-1210-10P: 78W

### D-Link Green Technology

- Power Saving: Enabled by default, save energy in 2 ways:

  - Sleep Mode: Drastically save power when the switch port link is down. For example, no PC connection or the connected PC is powered off.

  - Cable Length Detection: Detects the length of connected RJ-45 cables and adjusts power usage accordingly without affecting performance. Once the RJ-45 connection is less than 20m, the switch will reduce the power instead of full power, which is only needed for 100m cables.

- Time-based PoE function: Achieve power saving by shutting down power of devices during off working hours

**VLAN**

- 802.1Q VLAN standard (VLAN Tagging)
- Up to 256 static VLAN groups
- Asymmetric VLAN
- Management VLAN
- Auto-Voice VLAN

**QoS (Quality of Service)**

- 802.1p priority, DSCP priority queue mapping
- Up to 4 queues per port
- Supports Strict / WRR mode in queue handling
- Bandwidth Control

**Security**

- 802.1X port-based access control
- Port Security
- IP and MAC ACL
- Broadcast Storm Control
- D-Link Safeguard Engine
- Trusted Host

**Management**

- Web-based GUI or SmartConsole Utility
- D-Link proprietary CLI
- SNMP support
- PoE
- LLDP
- DHCP client
- Trap setting for destination IP, system events, fiber port events, twisted-pair port events, PoE Power On/Off events, PoE Power Error events and PoE over max power budget events
- Port access control
- Web-based configuration backup / restoration
- Web-based firmware backup/restore
- Firmware upgrade using SmartConsole Utility & Web-based management
- Reset, Reboot

## *Appendix C – Rack mount Instructions*

Safety Instructions - Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

D-Link
Building Networks for People